NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

KEY TERRAIN: APPLICATION TO THE LAYERS OF CYBERSPACE

by

Nicholas T. Pantin

March 2017

Thesis Advisor: Wade Huntley
Second Reader: Duane Davis

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE KEY TERRAIN: APPLICATION TO THE LAYERS OF CYBERSPACE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Nicholas T. Pantin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The concept of key terrain is a common fixture in military strategy and tactics. The emergence of cyberspace, with characteristics unseen in any warfighting domain, challenge the concept's value. This work is a conceptual analysis that examines the applicability of key terrain in the cyber domain. To determine if key terrain applies in cyberspace, we examine key terrain in traditional physical warfighting domains to understand the concept and draw comparisons. Each of the three layers of cyberspace is examined to determine if the concept of key terrain applies and to identify challenges presented when applying the concept. The result of this work finds key terrain to hold value and applicability within cyberspace. Key terrain can be found at each layer of cyberspace but with some considerations. Cyber key terrain requires constant reassessment, exists only under certain conditions, and can present difficulties in terms of measuring seizure and retention of terrain in cyberspace. The conclusion additionally finds that while cyberspace is unique, it does not require a cyber-specific key terrain definition. We recommend that changes be made to future doctrine, institutional education, and leader development in an effort to provide clarity when using traditional military concepts such as key terrain in cyberspace.

14. SUBJECT TERMS key terrain, cyber, doctrine, cyber key terrain	**15. NUMBER OF PAGES** 83
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89) Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

KEY TERRAIN: APPLICATION TO THE LAYERS OF CYBERSPACE

Nicholas T. Pantin
Captain, United States Army
B.S., Keiser University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2017

Approved by: Wade Huntley, Ph.D.
Thesis Advisor

Duane Davis, Ph.D.
Second Reader

Cynthia Irvine, Ph.D.
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The concept of key terrain is a common fixture in military strategy and tactics. The emergence of cyberspace, with characteristics unseen in any warfighting domain, challenge the concept's value. This work is a conceptual analysis that examines the applicability of key terrain in the cyber domain. To determine if key terrain applies in cyberspace, we examine key terrain in traditional physical warfighting domains to understand the concept and draw comparisons. Each of the three layers of cyberspace is examined to determine if the concept of key terrain applies and to identify challenges presented when applying the concept. The result of this work finds key terrain to hold value and applicability within cyberspace. Key terrain can be found at each layer of cyberspace but with some considerations. Cyber key terrain requires constant reassessment, exists only under certain conditions, and can present difficulties in terms of measuring seizure and retention of terrain in cyberspace. The conclusion additionally finds that while cyberspace is unique, it does not require a cyber-specific key terrain definition. We recommend that changes be made to future doctrine, institutional education, and leader development in an effort to provide clarity when using traditional military concepts such as key terrain in cyberspace.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APT	advanced persistent threat
ARPANET	Advanced research project agency network
AUSA	Association of the United States Army
BFT	Blue Force Tracking
BIOS	Basic input/output system
BMDS	ballistic missile defense system
CJA	Crown Jewels Analysis
CO	cyberspace operations
COA	course of action
COP	common operating picture
D-Day	June 6, 1944
DCO	defensive cyberspace operations
DDoS	distributed denial of service
DMZ	demilitarized zone
DNS	domain name server
DOD	Department of Defense
DODIN-OPS	Department of Defense information network operations
EMS	electromagnetic spectrum
FM	Field Manual
GPS	Global Positioning System
IOT	Internet of Things
IP	Internet protocol
IPB	intelligence preparation of the battlespace
IPV6	Internet Protocol Version 6
IT	information technology
JFC	Joint Force Commander
JFHQ-DODIN	Joint Force Headquarters—Department of Defense information network operations
JIPOE	Joint Intelligence Preparation of the Operational Environment
JP	joint publication

LOC	line of communication
METT-TC	mission, enemy, terrain and weather, troops and support available,
OAKOC	observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, cover and concealment
OCO	offensive cyberspace operations
PII	personally identifiable information
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment and time
SAMS-E	Standard Army Maintenance System - Enhanced
SATCOM	satellite communications
SCADA	supervisory control and data acquisition
SLOC	sea lines of communication
SQL	structured query language
TCP	transmission control protocol
	time available, and civil considerations
URL	uniform resource locator
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USJCS	United States Joint Chiefs of Staff

ACKNOWLEDGMENTS

I would like to thank Dr. Wade Huntley and Dr. Duane Davis for their guidance and assistance on this thesis. I want to thank Chloe Woida of the Graduate Writing Center for her assistance in helping me to decipher what I was trying to say. I would like to thank all the professors that I have had the opportunity to learn from. Each and every one of you provided some piece to this work. Last but not least, I want to thank my wife, Kelsey, for her love and support. You allow me to do great things and I appreciate you listening to my talks about abstract concepts in complex environments.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Admiral Michael S. Rogers, while addressing the House Committee on Armed Services in March 2016, described the mission of the then newly formed JFHQ-DODIN "to oversee the day-to-day operation of DOD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses" (Hearing to receive testimony on U.S. Strategic Command, 2016). While addressing an audience at the 2016 AUSA conference on potential vulnerabilities posed to military information systems, the vice chief of staff of the Army, General Daniel Allyn stated, "Commanders and Soldiers must know their key cyber terrain, understand the risk at each level, where essential data resides, and take necessary steps to reduce the threat" (Allyn, 2016, para. 15). These examples of military leaders using the term "cyber key terrain" demonstrates the use of traditional military vocabulary, concepts, and doctrine when discussing cyberspace. At first thought, this inherently makes sense as these concepts and processes have been used, integrated, and tested over the course of the U.S. military's history. The term "key cyber terrain" is something of a buzzword within the military leading one to automatically accept its functionality and fit in cyberspace. However, careful analysis may potentially determine instances in which these concepts have no meaning or lack applicability to the cyber domain. Understanding of key terrain and the environment of cyberspace presents questions: What exactly is cyber key terrain? Where or how, is it identified? Does the concept traditionally used to identify geographic and manmade structures mesh with the nonphysical environment of cyberspace?

Though its use is prevalent, many questions have potentially not been addressed as needed to ensure a common understanding of the concept of key terrain in cyberspace. This thesis will examine the question of whether the traditional military concept of key terrain can be adapted to the cyber domain, and if so, how that can be achieved.

A. FOCUS AND RESEARCH QUESTION

The focus of this thesis is to examine whether the traditional concept of key terrain has applicability in the cyberspace domain. This research will examine a doctrinal concept traditionally used in physical domains and determine how it applies to the non-physical layers of cyberspace (logical and cyber persona). To make this determination it is necessary to answer secondary research questions to scope the overall research question. First, why is key terrain in the physical domains important to military operations? Second, what is cyberspace and why is it important to the U.S. military? Last, does the concept of key terrain adequately apply to the non-physical layers of cyberspace? These questions will guide this thesis and help answer the overarching research question of whether the traditional military concept of key terrain can be adapted to the cyber domain, and if so, how that can be achieved.

It is important to understand that two of the chapters of this thesis will provide necessary background information and doctrinal understandings to frame the final assessment of applying key terrain to cyberspace. These chapters are meant to appeal to divergent audiences who may not have a complete understanding of either the concept of key terrain or the cyber domain and why these two are important to the DOD. These chapters will reference known material but with a focus on cyber key terrain.

B. PURPOSE AND IMPORTANCE OF RESEARCH

Major General Stephen Fogerty, the former commanding General of the Army's Cyber Center of Excellence, explains that "to win in a complex world, we must dominate the cyber domain" (U.S. Army Cyber Center of Excellence, 2015, para. 4). The ability to establish and maintain dominance in the cyber domain will heavily rely on foundational doctrine to instruct and guide the future cyber warriors of the U.S. military. Efforts to examine the applicability of existing doctrine and strategies to the cyber domain is essential to ensuring that current doctrine and strategies maintain relevance in cyberspace. Some concepts may have no place or meaning in cyberspace, while others may require refining or adjustment to meet the environment of cyberspace.

This thesis will search for the concept of key terrain's existence in the cyber domain to determine its application and value. In doing so, this research will explore what refinements or considerations must be taken into account to effectively integrate the concept into the cyber domain. With such analysis and understanding, the concept of cyber key terrain can provide beneficial effects to the cyber domain and cyber operational planning.

The importance of this research is that it contributes to an area in which limited scope of attention has been placed. This thesis will contribute to the body of research by examining a concept that many misunderstand or overlook in the cyber domain. Understanding cyber key terrain will better enable commanders to identify and prioritize assets and objectives for both defensive and offensive cyber operations. The importance of this research is hinged upon the fact that doctrinal processes and training will ultimately contribute to the success of the U.S. military achieving cyber dominance.

C. LITERATURE REVIEW

Despite the lack of literature on cyber key terrain, there are varying opinions on what cyber key terrain means, how it is defined, and whether it applies to cyberspace. Four relevant themes emerge in the literature review. First, there is no definitive cyber key terrain definition but rather a collection of definitions. The DOD, scholars, and private sector experts offer conflicting definitions and interpretations of the concept. Second, examples of cyber key terrain tend to focus on physical rather than the nonphysical manifestations. Using mainly physical manifestations may be the result of the instinctual habit of relating key terrain to physical properties. Third, confusion surrounds the use of multiple terms that are used interchangeably with key terrain. While these terms are similar, they have different meanings depending on type of operations and contexts. Last, while most analytical works accept the concept of key terrain in cyberspace without question, a few works suggest that the concept does not have applicability to the cyber domain. Furthermore, this perspective highlights that while works accept the concept in cyberspace, the discussion on how cyber key terrain is specifically applicable to the cyber domain is missing or not clearly captured.

1. Lack of Definition for Key Terrain in Cyberspace

A prevailing DOD definition of "cyber key terrain" does not exist. Joint Publication 3–12, *Cyberspace Operations*, is the joint doctrine publication that governs military activities and offers guidance for planning in cyberspace. Its purpose is to provide "military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs), and prescribes joint doctrine for operations and training" (United States Joint Chiefs of Staff [USJCS], 2013a, p. i). JP 3–12, defines key terrain as "any locality or area, the seizure or retention of which affords a marked advantage to either combatant" (p. II-10). This defines the concept of key terrain in the physical domain. This same definition is consistently found throughout military doctrine regardless of branch of service. However, no military doctrine, including JP 3–12, provides a definition for the concept of "cyber key terrain." While JP 3–12 does not define cyber key terrain, it does state that key terrain in cyberspace "involves network links and nodes that are essential to a particular friendly or adversary capability" (p. II-10). "Network links and nodes" offer a vague description when defining key terrain in cyberspace. JP 3–12 stresses the importance of key terrain in cyberspace but does not clearly explain what it is within the layers of cyberspace or how it can be identified. One potential hypothesis for this missing definition could be the DOD's belief that the current key terrain definition serves as a fitting definition in cyberspace despite its non-physical terrain. Another potential hypothesis could be the constantly changing environment of cyberspace does not allow for a definitive definition.

Outside of doctrine, various authors have attempted to define cyber key terrain. Raymond, Conti, Cross, and Nowatkowski (2014) acknowledge the fact that military doctrine does not define either "cyber terrain" or "cyber key terrain" and instead offer their own definitions. They refer to cyber terrain as "the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace" (p. 290), and define cyber key terrain as "systems, devices, protocols, data, software, processes, cyber personas, or other network entities, the control of which offers a marked advantage to an attacker or defender" (p. 294). Raymond et al.'s definition is far less vague than the doctrinal examples and presents

non-physical attributes like protocols, data, and cyber personas as the terrain features of cyberspace that could potentially be identified as key terrain.

Hobbs (2007) defines what he calls digital key terrain as “any network feature that, if controlled, will provide a tactical advantage” (p. 4). He concludes that “this will be based on the layout of the target, and the target’s network, but there will always be a few features that constitute key terrain” (p. 4). The definition is succinct but broad, as use of the term ‘network feature’ implies a vast number of things but does not specify the non-physical manifestations of cyberspace. However, Hobbs does support standard tactics and methodologies being applied to cyberspace and uses the tactical planning tool OCOKA, a mnemonic used for terrain analysis in the military, to demonstrate its usefulness in the cyber domain.

Kern (2015) defines cyber key terrain “as any physical, logical, or persona element of the cyberspace domain, including commercial services, the disruption, degradation, or destruction of which constricts combat power, affording a marked advantage to either combatant” (p. 13). His definition suggests the fact that key terrain could potentially exist in different layers of cyberspace. Kern presents the fact that key cyber terrain will rarely be in the control of the joint force, which is unlike any other warfighting domains. To demonstrate this lack of control, Kern uses the example of the inability to militarize and protect cyberspace in a way that the air space of the U.S. was following the 9/11 terrorist attacks.

“Key Defensive Terrain in Cyberspace: A Geographic Perspective” by Pingel (2003) focuses on a comparison of fortifying cities and computer networks. In doing so, Pingel provides three examples “firewalls, bastion hosts, and DMZs” and relates them to the physical manifestations used to protect cities (p. 4). Pingel defines terrain as encompassing “the irregularities and configuration of the medium of conflict in whatever forms it may take” and defines key terrain using the definition in U*.S. Army Operations Manual* (now currently FM 3–0) (p. 2). Pingel is one of the few authors to present an accepted doctrinal definition as the basis for defining key terrain in cyberspace. He presents the importance of the understanding of key terrain by stating “the success of an

attack on, or defense of, a network depends heavily on how well key terrain of the network is understood and incorporated" (p. 4).

Riley (2014) defines key terrain in cyberspace as "key assets, accounts, data, etc.," asserting that a loss of these items to a threat actor would render a significant defeat to a defender (para. 27). His definition is simplistic; however, it does acknowledge non-physical cyber terrain characteristics such as accounts and data. This is yet another example that demonstrates the lack of prevailing or accepted "cyber key terrain" definition.

In contrast to such attempts to define cyber key terrain, others see the traditional doctrinal definition as sufficient. Lanham (2012) suggests the need to maintain traditional military vocabulary when discussing warfare in the cyber domain. Lanham argues the best approach "is to use the military decision making process, augmented with doctrinal Joint and Army graphics, and treat cyber terrain approximately the same as we treat the land and air domains" (p. 7). His article contributes to the argument that communicating key terrain in cyberspace will be better received if use of accustomed planning processes, terms, and tools are maintained. Lanham presents this exact point stating, "instead of using the civilian-dominated language of enclaves, intrusion detection systems, and firewalls, use *Joint Publication and Field Manual* 1–02 language such as sensor, positions, strong points, LOCs, communications zones, deliberate defense, and deliberate operations" (p. 9). Lanham suggests that using existing vocabulary "is more likely to retain the interest, understanding, and resource commitment of commanders than by 'going geek' on them" (p. 11). In addition, Lanham supports his conclusion stating that he "has not seen evidence in the classified or unclassified realms that convince him of the added value of creating unique-to-cyber processes and vocabulary" (p. 11).

Williams (2014) agrees that current doctrine may suffice, stressing "established joint doctrine accommodates operations in cyberspace quite well, so we do not need to invent anything new. USCYBERCOM staff has found that there are few adjustments required to integrate cyberspace operations into existing planning and execution processes" (p. 13). Williams point supports the argument that the invention of a new definition may not be necessary as current doctrine applies to cyberspace.

Applegate, Carpenter, and West (2017) additionally support this conclusion stating that "there is no need to create a separate definition for cyber key terrain, as the joint definition for key terrain is adequate and applicable across all domains" (p. 22). This argument supports the fact that despite the differences and non-physical attributes of the cyber domain, the concept of key terrain applies and requires no different definition. Additionally, Applegate et al. argue that previous efforts are flawed in their methodologies in regards to three assessments. "First, in almost every case, the researchers focused on what items should be considered key terrain rather than on how to identify key terrain in a contextual manner. Second, previous efforts omitted the planning concepts of objective and mission, which are essential to identifying key terrain for a military operation. Finally, these efforts often confused or misidentified key terrain with critical assets" (p. 19).

Taking these analyses as a whole, there is clearly no strong consensus on the meaning of the concept of key terrain in cyberspace. This analytical uncertainty forms the backdrop for the absence of a single DOD definition. However, in this conceptual discussion some trends are apparent, as the following sub-section discusses.

2. Emphasis on Physical Network Layer

There is a notable theme of literature advocating for the use of "cyber key terrain," most works do not effectively identify or pay attention to the non-physical layers of cyberspace. Instead they tend to gravitate toward physical layer examples. The abundance of literature using examples of mainly physical manifestations as cyber key terrain may drive that lack of a prevailing definition.

Hobbs (2007) uses the example of "last hop routers, domain controllers and internal hosts" when describing key terrain, which demonstrates physical layer manifestations (p. 4–5). Mills (2012) identifies what he terms "earthly manifestations" that include "data centers, commercial Internet service providers, undersea cables, International Standards bodies, BIOS, supply chain, cyber workforce, and innovation as key terrain elements that show significant pressure points for Cyber" (p. 100). Mills suggests that despite cyber being the land of "one's and zero's" it still has physical

manifestations that include data centers and undersea cables and stresses that "assuming the cyber domain may free us of traditional Clausewitzean key terrain concepts … is a faulty logical starting point because Cyber does have physical manifestations" (p. 99).

Dressler (2015) presents the fact that cyber key terrain identification "includes all critical information, systems, and infrastructure; whether owned by the organization or used in transit by its information" (p. 49–50). This again demonstrates physical layer manifestations, with the "in transit" possibly referring to data or logical information sent through transmission. Regardless, this does not specify the non-physical properties that will most likely be encountered in cyberspace. Dressler does present a hypothetical operational case study, in which a Joint Task Force Commander designates his logistical support information systems as cyber key terrain (Dressler, 2015). While the example was not intended to specify cyber components and their layers, this example ignores the specificity that key terrain in cyberspace requires. For example, better identification of key terrain may be the administrative level accounts (cyber persona) or IP addresses and resident data (logical layer) rather than the system as a whole.

Thomas (2014) addresses the potential qualities of a cyber strategist and proposes curriculum areas needed to educate and train cyber strategists of the future. Thomas describes terrain in which a cyber strategist must consider such as "optical fiber, Internet service providers (ISPs), routers, switches, wireless links, terrestrial gateways and underwater cables of all types, satellites, power stations, and many other features often described as tubes, both visible and invisible" (p. 379). All of these examples demonstrate physical manifestations. Thomas does not offer cyber key terrain examples but alludes to key terrain, stating that cyber terrain features "must be protected and monitored, but they also represent key areas of influence or manipulation" (p. 379).

"Awaiting Cyber 9/11" by Magee (2013) discusses the need for a cyber strategy that includes legislative development on cyber security, protection of critical infrastructure, and additional authorities to DOD in order to execute cyber defense. Magee proposes that in protecting critical infrastructure, use of a cyber common operating picture (COP) would be effective. While discussing the potential for a COP, Magee references the Armed Forces focus of selecting, capturing, and retaining key

terrain (Magee, 2013). Magee asserts that “Similarly, the cyber COP would focus on key cyber terrain. The cyber terrain would need to be a prioritized list of key nodes that encompass the .gov, .mil, and .com domains” (p. 80). The visibility provided by key terrain would assist in the overall situational awareness required of the cyber domain (Magee, 2013). A prioritized list of key nodes is organic to the physical layer. The prioritized list of key nodes presented by Magee lacks the inclusion of non-physical cyber terrain elements that may be identified as key in order to better enhance situational awareness.

Despite the abundance of physical layer examples there are some that acknowledge the potential for non-physical manifestations as key terrain. One such example is seen by Kieffer (2016) in which he uses an administrative account (cyber persona layer) as an example of key terrain, while comparing and contrasting the IPB processes usefulness in the cyber domain. Kieffer argues that, “Control over an administrative account grants access to new ‘area’ and ‘structures’ thus helping espionage and therefore an ‘area-of-influence’” (p. 4). This example demonstrates a non-physical cyber layer element (admin account) owning the attributes of key cyber terrain.

Brigadier General George J. Franz III (2012) describes the potential for cyber key terrain to be such elements as fiber optic cable, satellite communication (SATCOM) uplink/downlink, subnets, databases with usernames and passwords, and technicians. Franz description presents some non-physical attributes of cyberspace but also includes people. Franz states that “key terrain applies to those physical and logical elements of the domain that enable mission essential warfighting functions” (Franz, 2012, slide 7). This was additionally referenced as the definition of cyber key terrain in a MITRE technical report on “Mapping the Cyber Terrain” by Bodeau, Graubart, and Heinbockel (2013).

Williams (2014) furthers demonstrates the nonphysical nature of key terrain by representing the potential for multi-layer existence for key terrain in cyberspace. Williams supports the argument that cyber key terrain is more than just one feature or object; it more than likely consists of various layers and dependencies. Williams, using the Ballistic Missile Defense System (BMDS) as a key terrain example, demonstrates the complexity and robustness of key terrain in the cyber domain. In the context of a DCO

mission, Williams uses a scenario of a commander identifying the BMDS to his staff as key terrain. Williams suggests the next step is to "technically enumerate the key cyber terrain from sensor to shooter" (pp. 15–16). For the BMDS, Williams asserts that there is a need to understand and view the system in its entirety, thus it will include all the "various sensors that collect launch data and the networks and systems that move that data to a variety of command centers for attack assessment" (p. 16). This demonstrates the end-point to end-point assessment that must be done, more commonly referred to as "sensor to shooter." The intricate network of the BMDS opens the door for potential weaknesses from multiple attack vectors. From a DCO perspective Williams suggests that "there are more vulnerabilities than we can address, and therefore we must prioritize our efforts against adversaries with specific capability and intent to interfere with our key cyber terrain" (p. 16).

Thus, a few assessments open the door to thinking about how the concept of key terrain might extend to nonphysical dimensions of cyberspace. These assessments fall short of applying the key terrain concept to nonphysical cyberspace systematically or confronting the challenges of translating an intrinsically physical concept to this application.

3. Confusion of Terminology

There are various terms both within the military and private sector that are used interchangeably with key terrain. One example is seen by Riley (2014) when he defines key terrain and uses the term "crown jewels analysis." After defining key terrain Riley states "within the cybersecurity world this [key terrain] is generally known as Crown Jewels analysis" (para. 27). This is potentially incorrect and more importantly a cause for confusion. Riley goes on to associate critical assets as key terrain stating, "By looking at the critical assets [key terrain] within the defender's cyber terrain, through techniques such as crown jewels analysis, and then determining who would want those assets and why, defenders can better understand the kinds of threat actors that they are likely to face, the patterns of attack associated with those types of threat actors, and ultimately the weaknesses, vulnerabilities, and configuration issues that are likely to be exploited in an

attack" (Riley, 2014, para. 29). In this excerpt, Riley interchangeably uses "key terrain," "critical assets," and "crown jewels." One cannot say this is a flaw as the understanding of key terrain appears to vary among authors and the military, but it does suggest that there are some misinterpretations or misunderstandings of the concept of key terrain.

While presenting the facts of what may be the first documented Cyberwar, Hollis (2011) concludes with a lesson on the need for cyber targets to be identified and access developed prior to any military operations. Hollis presents the argument that "identifying and then monitoring the health of national critical infrastructure or 'key terrain' in cyberspace (ex: government networks; critical communications nodes; national-level power, financial, and health networks; selected media outlets; and vital enclave networks) are critical to providing advanced warning of aggression" (Hollis, 2011, p. 6). In his point, Hollis equates critical infrastructure and key terrain as the same thing. This may again not be a flaw but does pose some confusion as to whether the two are actually the same.

The argument of misuse of the term "key terrain" was additionally pointed out by Applegate et al. (2017) who argue that the imprecise use of terms such as "critical assets," "crown jewels," and "key terrain" implies a lack of understanding of the concept. This misunderstanding of the concept was additionally presented by Dressler (2015). Dressler references the point that there may be a gap in the understanding of cyber key terrain with the commanders at the higher echelons. Dressler suggests that "strategic and operational commanders do not know or fully understand how to determine their cyber key terrain. If they do, typically, they have not taken the required actions or time to determine and designate cyber key terrain" (p. 54). Whether true or not this demonstrates yet another argument supporting a gap in the understanding of the concept in cyberspace.

4. Questioning Key Terrain's Application in Cyberspace

Some challenge or question altogether the applicability or usefulness of the concept of key terrain in the cyber domain. Libicki (2012) describes what he calls "conceptual errors that may arise by thinking of cyberspace as a warfighting domain analogous to the traditional warfighting domains" (p. 322). He references the example of

"key terrain" questioning whether it holds value in cyberspace. Libicki argues that while it is true of any network to have some physical nodes and services that are more important than others, their ownership may result in an empty victory, due to the malleability of cyberspace such as software (Libicki, 2012). He is alluding to the fact that ownership in cyberspace may not be an obtainable or measurable feat and adds that "offensive cyberspace operations generally cannot break physical nodes and the services provided by networks can be and are increasingly virtualized" (p. 332–333). Libicki asserts that he is not dispelling the concept but questions the concept's true accuracy in the cyber domain. He concludes by presenting the fact that the ground warfare metaphor of "key terrain" may be misleading especially at the more senior officer levels (Libicki, 2012).

Gioe (2016) asserts that "in land warfare, identifying, seizing and holding key terrain is of critical importance" and this same concept remains true in the cyber domain (Gioe, 2016, para. 3). Gioe argues that while the concept remains true in cyberspace there are also caveats. "First, cyber operations can help commanders actually change some of the virtual key terrain itself. Secondarily, unlike land warfare, cyber operations can be present on key terrain (and perhaps hold it) without the enemy identifying this presence, or understanding its hold over the key terrain. In this sense, the maneuver principle of observation can be both closer and concealed in the virtual realm" (Gioe, 2016, para. 3).

5. Layer Composition of Cyberspace

Another notable point of contention is the fact that there are multiple perspectives on the layer composition of cyberspace. JP 3–12 describes three layers, but other works see additional layers, which may ignite misunderstandings of the concept or be the result of varying definitions.

Shawn Riley's cyber terrain model is built off of the DOD's efforts representing the physical and virtual layers while additionally representing the full triangle of sustainment or the three pillars of cybersecurity: People—Organizations & Processes—Technology (Riley, 2014). Riley argues the need for a model that represents both physical, real-world, and virtual layers of cyberspace (Riley, 2014).

Raymond, Conti, Cross, Nowatkowski (2014) describe cyberspace as five planes rather than DOD's three layers. However, three of the planes relate exactly to the three layers of JP 3–12. Raymond et al. offer real world examples of potential objects that fall into these layers/planes. Raymond et al. describes "a poorly configured wireless device that uses an obsolete security protocol" as potential key terrain at the physical plane (p. 295). At the logical plane, they use the example of key terrain as "the Domain Name System (DNS), which provides logical mappings between domain names (such as www.ccdcoe.org) and their Internet Protocol (IP) addresses (such as 195.222.11.253)" (p. 295). At the cyber persona plane they identify key terrain as "a system administrator's account ... if possession of that account could be used by an attacker to compromise a defender's resources" (p. 295). Raymond et al. additionally present the fact that "even an unprivileged user account could be key depending on the owner of the account" (p. 295). Based on the literature for this review, Raymond, Conti, Cross, and Nowatkowski are the only authors that present clear examples of what they consider key terrain at each cyberspace layer.

6. Cyber Key Terrain Is Relevant

Despite the varying opinions and understanding of cyber key terrain, the most common theme found among the literature suggests that the control and understanding of cyber key terrain is essential to the defensive posture of the U.S. military in the cyber domain. Additionally, there is support for the assessment and update of cyber doctrine as it too is necessary for the success of the U.S. military.

Winterfeld (2001), recognizing the speed at which technology is advancing, suggests that "as the U.S. Army transitions into the digital age it is imperative to determine how to port their analog doctrine or business processes into a digital doctrine that moves at the speed of the Internet" (p. 8). Winterfeld, in the context of IPB doctrine, champions the idea that current doctrine should be readdressed and developed to capture the changing environment of cyberspace. In addition to development of cyber IPB doctrine, Winterfeld suggests updated doctrine be integrated into training installations and exercises to ensure leaders are ready to use it during the next conflict.

Pingel (2003) additionally sees the importance of key terrain in cyberspace. Pingel suggests that "the success of an attack on, or defense of, a network depends heavily on how well key terrain of the network is understood and incorporated" (p. 4). Mills (2012) argues that "critical cyber terrain must be controlled, or at least decisively influenced, to maintain relevancy in contemporary cyber and to help build the future path and direction of cyber. … The cyber domain is subject to the role of key terrain just as the legacy domains of the past" (p. 105). Lewis (2016) stresses that "knowing cyber key terrain not only enables offensive maneuver also provides additional disruption to the enemy's intrusion kill chain in cyberspace by limiting at least one step in the payload delivery" (Lewis, 2016). Riley (2014) presents the point that finding key terrain allows for the defender to better understand threat actors, patterns of attack, and ultimately weaknesses, vulnerabilities, and configuration issues that may be exploitable.

The point that all of these authors make is that key terrain has relevance and importance in the cyber domain and that efforts to better understand and educate leaders in the military is necessary to achieve defensive goals in cyberspace.

D. METHODOLOGY

This thesis is a conceptual analysis of a question that relies on the understanding of the concept of key terrain and the cyber domain. In drawing upon military doctrine, this thesis will use the DOD's definition of the concept of key terrain as the foundational base when discussing the concept in cyberspace. In regards to the composition of cyberspace this thesis will accept the three-layer composition of cyberspace defined by the DOD. Before analyzing the concept of key terrain in cyberspace, it is necessary to understand key terrain in military strategy and tactics. Key terrain is explained using military doctrine in order to understand the conditions needed for its use. Before applying the concept of key terrain to cyberspace, it is necessary to understand the composition of cyberspace, how it works and why the military is dependent on it for operations. This requires the examination of military cyber doctrine, scholarly literature on the functionality of cyberspace, and examples of military dependence on cyberspace.

To apply key terrain to cyberspace, analysis of key terrain application at each layer is required. This evaluation identifies if the concept fits in the layer, where it fits, and potential challenges or constraints to applying. This is done at each layer in order to assess the overall application of key terrain in cyberspace. The analysis of the application will also examine the need for a cyber-specific key terrain definition to see if it will help or hinder efforts to clarify key terrain in cyberspace. The research and secondary questions are answered once a clear understanding of the concept of key terrain, the cyber domain, and key terrain's application within the layers of cyberspace is achieved.

E. THESIS OVERVIEW

This thesis is composed of five chapters in total. The focus and intent of each chapter is as follows:

Chapter I frames the current problem, outlines the research question for this thesis, and provides a literature review to identify any limitations or short falls that exist in the area of study.

Chapter II examines the concept of key terrain in physical domains, focusing on the concepts use in military operations and the processes and frameworks used to identify its existence. The purpose of this chapter is to demonstrate why key terrain is important to military operations and planning and create the understanding of key terrain variances in other domains.

Chapter III explores the emergence of cyber as a new war-fighting domain. Chapter III provides the introduction to the cyberspace domain, its environment, multi-layer terrain composition, and the dependence the DOD has on cyberspace to conduct military operations. The purpose of this chapter is to identify cyberspace from a military perspective and how it is important to U.S. military operations.

Chapter IV examines the application of the concept of key terrain to the cyber domain. This chapter focuses on how cyber key terrain is defined and determines whether the concept applies at all, and if so, at which layer(s). Additionally, this chapter examines

what key terrain is not and the potential issues or challenges that result from its application or lack of application.

Chapter V concludes with the final assessment of whether or not the concept of key terrain adapts to the cyber domain. This chapter summarizes the overall findings of the research question and secondary questions. Chapter V recommends any further research or areas of study that will assist in the continued understanding of key terrain in cyberspace and any policy implications that may arise.

II. KEY TERRAIN IN THE PHYSICAL DOMAIN

> Terrain and weather are neutral; they favor neither side unless one is more familiar with—or better prepared to operate in—the physical environment.
>
> —Department of the Army (2008, pp. 5–6)

A. INTRODUCTION

Terrain commonly refers to an area of land and its physical features. The effects, advantages, and disadvantages of these physical features are closely examined in order to determine the proper military strategies, tactics, and capabilities to achieve success on the battlefield. Analysis of the battlespace terrain is essential to military planning as it will guide a commander on decisions such as where to maneuver or position forces, where to set up communication links, or where logistics routes will be located. In order to answer these questions the commander requires an understanding of the physical terrain and the overall operational environment. This analysis is necessary regardless of the type of mission or area of operations and serves as a critical ingredient to proper mission planning and execution.

Ultimately there are certain terrain features that will stand out, as they provide an advantage or are determined as necessary to control in order to succeed with a mission. The commander seeks to locate these key terrain features in order to integrate them in to the military planning process and secure them to ensure the success of his or her forces. “Key terrain” fittingly serves as the term identifying the terrain that yields probable advantage and success. Its importance in the military dates back some time and whether realized or not the concept has played a part in every major battle. These battles have been waged in the physical land, air, and maritime domains. Using key terrain in the cyber domain will undoubtedly display some variances to the other domains. A clear understanding of key terrain’s history, military importance, and application to the physical domains of land, air, sea, and space will provide the foundational understanding needed for application to the cyber domain. To understand the term “cyber key terrain” one must first understand “key terrain” on its own.

B. DOCTRINAL ORIGINS OF KEY TERRAIN

Terrain's influence on military tactics and strategy is noted as far back as the ancient Chinese General Sun Tzu and more recently in the 19th century by the great Prussian military strategist, Carl Von Clausewitz. The doctrine of the U.S. military heavily adapts the strategies of these notable military strategists, and their teachings provide much of the foundational framework upon which U.S. military doctrine is built.

Clausewitz's influential work *On War* dedicates two chapters to terrain. Clausewitz describes how "geography and ground can affect military operations in three ways: as an obstacle to the approach, as an impediment to visibility, and as cover from fire" (Clausewitz, 1976, p. 348). Clausewitz saw the potential for using terrain to obstruct an enemy's movement, affect their visibility, and provide protection from attack. Not only did Clausewitz acknowledge the importance of terrain and how its understanding plays on the battlefield but he also distinguishes that terrain offers advantages to he who controls it. Clausewitz describes this advantageous terrain as the "high ground" and cites what he calls "three obvious reasons" to the benefits of holding this ground. "First, the high ground always inhibits the approach; second shooting downward is perceptibly more accurate than shooting upward; and third, heights command a wider view" (Clausewitz, 1976, p. 352). Clausewitz believed that this high ground was essential to success on the battlefield stating, "No army is capable of maintaining a position in the valley of a major river if it does not command the surrounding heights" (Clausewitz, 1976, p. 354). Clausewitz not only saw an advantage from the military tactics perspective but also an advantage in regard to the morale of the force that controlled it. Clausewitz believed that the superiority and security that one holds by gaining control of the high ground may additionally offer more confidence that impresses the mind more acutely than the circumstances that modify them, serving as an additional reason to control the high ground (Clausewitz, 1976). Clausewitz saw the importance that the high ground presented in battle and stresses that it must be analyzed and accounted for when implementing strategies of war. His observations serve as the basis of what is known as key terrain in U.S. military doctrine today. The DOD has adopted much of Clausewitz's strategy and specifically identifies key terrain in multiple doctrinal publications.

C. HOW THE DOD DEFINES KEY TERRAIN

The Department of Defense defines key terrain as "any area the seizure, retention, or control of which affords a marked advantage to either force" (USJCS, 2009, p. II-13). It serves as the foundational definition among all the branches of service and is adapted within each of their individual doctrinal publications. Their adaptations to key terrain have some small alterations but it does not take away from the definition's meaning. For example, the Army and Marine Corps share doctrine on Intelligence Preparation of the Battlefield/Battlespace (IPB) which defines key terrain exactly as the DOD with only one subtle change using the term "combatant" instead of "force" (Department of the Army, U.S. Marine Corps, 2014). The wording of the definition remains similar despite the varying environments within the domains because key terrain is generally identified by geographic or man-made features making it easy to conceptualize.

There are considerations that determine when key terrain applies. First, key terrain is identified as a result of a mission or operation. Key terrain is a byproduct of the military planning process that occurs when there is an operation or desired effect needed. Without an operation and the guidance and intent of a commander there is just terrain. Second, there must be an adversary or enemy to inflict the desired effects upon. Key terrain is considered an advantage to whoever controls it and would imply that there is someone else (adversary) to compete for the terrain. Lastly, "key terrain is temporal. It changes with the mission and adversary. In the absence of either, these elements may be critical infrastructure or a key resource, but not key terrain" (Franz, 2014). Some additional considerations for key terrain are outlined in JP 2–01.3:

- Key terrain varies with the level of command. For example, a large city may represent an important objective to an operational-level commander, whereas a tactical commander may consider it to be an obstacle.
- Terrain which permits or denies maneuver, such as bridges or chokepoints, may be key terrain.
- Major obstacles rarely constitute key terrain. Thus, the high ground dominating a river, rather than the river itself, is considered key terrain.
- Key terrain may include areas and facilities that may have an extraordinary impact on mission accomplishment (e.g., theater ballistic

> missile launch facilities, cruise missile launch sites, airfields). (USJCS, 2009, p. II-14).

The U.S. Army uses another term called "decisive terrain," which specifies a type of key terrain. According to the Army's FM 3–90-1, "decisive terrain, when present, is key terrain whose seizure and retention is mandatory for successful mission accomplishment" (Department of the Army, 2013, p. 1–25). Like key terrain, decisive terrain is designated by the commander, communicated to the staff, and deemed critical as the friendly force must control it in order to successfully accomplish its mission (Department of the Army, 2013). While decisive terrain is initially identified as key terrain, careful consideration should be used when differentiating the two, as they are not exactly the same.

D. HOW IS KEY TERRAIN IDENTIFIED?

Key terrain is identified through a process known as terrain analysis. DOD doctrinal processes like Joint Intelligence Preparation of the Operational Environment (JIPOE) and the Army and Marine Corps IPB are examples of commonly used analytical processes in which terrain analysis occurs. Terrain analysis is not the end product of JIPOE or IPB, but its results fuel the commander's decision of identifying key terrain and will ultimately be communicated to all the staff during operational planning and courses of actions (COA) development. In addition to key terrain, terrain analysis may determine areas that are obstacles such as swamps, marshes, or dense forest. These areas may hinder maneuverability of land forces but may also serve as an area to funnel an adversary or use as protection for your flank. Terrain analysis examines the topology and geographic or manmade features of an area of operation to provide the vital intelligence needed. This ultimately provides the commander with the understanding of the operational environment.

1. Operational Environment

It is important to understand the operational environment because of its significance to decision making on the battlefield. "The operational environment is a composite of the conditions, circumstances, and influences that affect the employment of

capabilities and bear on the decisions of the commander" (Department of the Army, 2008, p. 1–1). Analysis of the operational environment is done using operational and mission variables. Army doctrine asserts that its leaders will, "plan, prepare, execute, and assess operations by analyzing the operational environment in terms of the operational variables and mission variables" (Department of the Army, 2011, p. 2). The operational variables help develop a "comprehensive understanding of the operational environment," while mission variables describe the area of operation and how "they might affect a mission" (Department of the Army, 2012, p. 1–7, 1–8). The operational environment is filtered through each of these variables in order to create situational awareness, understanding, and allow for mission refinement. Terrain and the physical environment serve as components for both operational and mission variables.

a. Operational Variables

Operational variables consist of eight interrelated operation components: political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) (Department of the Army, 2012). Each describes objects that influence operations and their specific descriptions can be seen in Figure 1. In terms of key terrain and terrain analysis the focus is centered on the physical environment variable. The physical environment consists of the "geography and man-made structures that reside in the operational area" (Department of the Army, 2008, p. 1–8). Some of the factors that could potentially affect the physical environment identified in FM 3–0, *Operations*, include:

- Man-made structures, particularly urban areas.
- Climate and weather.
- Topography.
- Hydrology.
- Natural resources.
- Biological features and hazards.
- Other environmental conditions. (Department of the Army, 2008, p. 1–8)

FM 3–0 additionally points out that the enemy understands these affects and will most likely opt for more complex and challenging terrains to engage in operations. "The degree to which each operational variable provides useful information depends on the situation and echelon" (Department of the Army, 2008, p. 1–9). Operational variables are ideal to higher level echelons when planning but are not discarded at the lower levels.

Variable	*Description*
Political	Describes the distribution of responsibility and power at all levels of governance—formally constituted authorities, as well as informal or covert political powers
Military	Explores the military and paramilitary capabilities of all relevant actors (enemy, friendly, and neutral) in a given operational environment
Economic	Encompasses individual and group behaviors related to producing, distributing, and consuming resources
Social	Describes the cultural, religious, and ethnic makeup within an operational environment and the beliefs, values, customs, and behaviors of society members
Information	Describes the nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information
Infrastructure	Is composed of the basic facilities, services, and installations needed for the functioning of a community or society
Physical environment	Includes the geography and manmade structures, as well as the climate and weather in the area of operations
Time	Describes the timing and duration of activities, events, or conditions within an operational environment, as well as how the timing and duration are perceived by various actors in the operational environment

Figure 1. Operational Variables.
Source: Department of the Army (2012, p. 1–7).

b. Mission Variables

Lower echelons at the tactical level use mission variables, due to their direct impact on the mission. These mission variables consist of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC) (Department of the Army, 2012). Descriptions for each of these variables are found in Figure 2. Focusing on the variable of "terrain," the intent is to understand the terrain as it "directly affects the selection of objectives and the location, movement, and control of forces" (Department of Army, 2008, p. 5–6).

Variable	*Description*
Mission	Commanders and staffs view all of the mission variables in terms of their impact on mission accomplishment. The mission is the task, together with the purpose, that clearly indicates the action to be taken and the reason therefore. It is always the first variable commanders consider during decisionmaking. A mission statement contains the "who, what, when, where, and why" of the operation.
Enemy	The second variable to consider is the enemy—dispositions (including organization, strength, location, and tactical mobility), doctrine, equipment, capabilities, vulnerabilities, and probable courses of action.
Terrain and weather	Terrain and weather analysis are inseparable and directly influence each other's impact on military operations. Terrain includes natural features (such as rivers and mountains) and manmade features (such as cities, airfields, and bridges). Commanders analyze terrain using the five military aspects of terrain expressed in the memory aid OAKOC: observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, cover and concealment. The military aspects of weather include visibility, wind, precipitation, cloud cover, temperature, humidity.
Troops and support available	This variable includes the number, type, capabilities, and condition of available friendly troops and support. These include supplies, services, and support available from joint, host nation and unified action partners. They also include support from civilians and contractors employed by military organizations, such as the Defense Logistics Agency and the Army Materiel Command.
Time available	Commanders assess the time available for planning, preparing, and executing tasks and operations. This includes the time required to assemble, deploy, and maneuver units in relationship to the enemy and conditions.
Civil considerations	***Civil considerations* are the influence of manmade infrastructure, civilian institutions, and activities of the civilian leaders, populations, and organizations within an area of operations on the conduct of military operations.** Civil considerations comprise six characteristics, expressed in the memory aid ASCOPE: areas, structures, capabilities, organizations, people, and events.

Figure 2. Mission Variables. Source: Department of the Army (2012, p. 1–9).

2. OAKOC

When examining terrain at the tactical level with the mission variables (METT-TC) the Army commonly uses the acronym OAKOC. This mnemonic uses five military aspects of terrain consisting of: observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, and cover and concealment (Department of the Army, 2012). When conducting this analysis, it must be done so from the perspective of both the friendly and enemy forces. OAKOC is beneficial in that it can be applied on the ground

using fundamental skills taught at the lowest levels in the Army. The Joint Publication for JIPOE (JP 2–01.3) defines the five military aspects of terrain as follows:

- **Observation and fields of fire—** "'Observation' is the ability to see (or be seen by) the adversary either visually or through the use of surveillance devices. A 'field of fire' is the area that a weapon or group of weapons may effectively cover with fire from a given position" (USJCS, 2009, p. II-11).

- **Avenues of approach—**"An avenue of approach is a route of an attacking force of a given size leading to its objective or to key terrain in its path" (USJCS, 2009, p. II-14).

- **Key terrain—**"Key terrain is any area the seizure, retention, or control of which affords a marked advantage to either force" (USJCS, 2009, p. II-13).

- **Obstacles—**"Obstacles are obstructions designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force. Obstacles can be natural, manmade, or a combination of both. These can include buildings, steep slopes, rivers, lakes, forests, swamps, jungles, cities, minefields, trenches, and military wire obstacles. An evaluation of obstacles leads to the identification of mobility corridors. This, in turn, helps to identify defensible terrain and avenues of approach" (USJCS, 2009, p. II-11).

- **Cover and Concealment—**"'Concealment' is protection from observation, and can be provided by features such as woods, underbrush, snowdrifts, tall grass, and cultivated vegetation. 'Cover' is protection from direct and indirect fires. It can be provided by such things as ditches, caves, tunnels, river banks, folds in the ground, shell craters, buildings, walls, and embankments. Areas with good concealment and cover favor both offensive and defensive COAs. Since concealment and cover are basically the inverse of observation and fields of fire, the analysis of all four of these categories should be integrated in order to (a) Identify defensible terrain and potential battle positions; (b) Evaluate avenues of approach; and (c) Identify potential assembly and dispersal areas" (USJCS, 2009, p. II-11).

When conducting terrain analysis there are many variables to take into account. Examining these variables, specifically the variables associated with the terrain and physical environment, will guide the identification of key terrain. Thus, far the identification process has been focused on the physical domains, but there may be

benefits to using terrain analysis tools and frameworks when identifying key terrain in cyberspace should the concept prove to be applicable.

E. KEY TERRAIN COMPARISON AMONG DOMAINS

When comparing key terrain among the domains there are some subtle differences that are the result of their variances in physical environments. Despite the variances between the domains, a trend can be seen in regards to certain terrain features that offer an advantage during a military operation. There is also a trend for key terrain to exist in one domain due to its strategic importance to another domain. This is most commonly seen in joint operations and during the D-Day invasion where multiple key terrain objectives were selected due to their seizure being necessary for air, naval, and land assets. For example, an amphibious assault may be necessary in order to secure a certain beachhead that allows land forces to aground or the capture of an airfield may be necessary to allow air assets the ability to maneuver.

There are currently five war fighting domains consisting of land, air, maritime, space, and cyberspace. The domains differ in their physical compositions and dimensions but they all rely on physical terrain and manifestations when identifying key terrain. Cyberspace notably challenges this with its domain's unique characteristics and will be detailed further in Chapter III. Key terrain examples between the various domains demonstrates just how its applicability transcends various environments.

1. Land Domain

The land domain is the most commonly referenced domain in terms of the concept of key terrain. It was the first warfighting domain before man navigated waters, skies and outer space. An example of key terrain in the land domain may be a hilltop overlooking a known enemy supply route. By positioning forces on the hilltop, certain advantages are gained that include cover, concealment, and the ability to observe the route. Should engagement with the enemy become necessary, the hilltop allows for concentrated fire on the target, and alternately serves as a disadvantage to an enemy orchestrating an uphill battle. The land domain also possesses man-made terrain features that can serve as key terrain if deemed necessary. An example of a man-made key terrain

feature could be a bridge serving as a single point of entry or bottleneck. If the bridge is the only point of entry or exit, then control of the bridge may be necessary to execute a blockade, prevent retreat, resupply, or reinforcement to the enemy. These two simplistic examples demonstrate the concept of key terrain within the land domain. It is important to understand that a hilltop or bridge is not key terrain just because it resides in an area of operation or battle space, it is considered key terrain because control of the area marks an advantage along with the ability to deliver additional desired effects.

2. Maritime Domain

The maritime domain consists of "the world's oceans, seas, bays, estuaries, islands, coastal areas, littorals, and the airspace above them" (USJCS, 2009, p. II-16). When planning maritime operations, there are certain key aspects that should be evaluated in order to identify key terrain from both the friendly and enemy perspectives. "Key military aspects of the maritime domain can include maneuver space and chokepoints; natural harbors and anchorages; man-made infrastructures; sea lines of communications (SLOCs), and ocean surface and subsurface characteristics" (USJCS, 2009, p. II-16). These key aspects are of importance, as they will help determine where potential key terrain may be located. JP2-01.3 offers the following real world examples of maritime key terrain; "The Strait of Gibraltar and Suez Canal due to their ability to control reinforcement or resupply operations in the Mediterranean Sea and Persian Gulf, air bases in Iceland that dominate the North Atlantic shipping lanes in mid-ocean, and Diego Garcia which serves as a maritime pre-positioning base to support joint operations in the Indian Ocean and Persian Gulf" (USJCS, 2009, p. II-20).

3. Air Domain

The air domain is defined as "the operating medium for fixed-wing and rotary-wing aircraft, air defense systems, unmanned aircraft systems, cruise missiles, and some theater and antitheater ballistic missile systems" (USJCS, 2009, p. II-20). Key terrain in the air domain is influenced by characteristics on land such as terrain or weather as they will influence maneuverability and capabilities of air assets. Therefore, key terrain could be any terrain feature that allows for freedom of maneuver and accessibility to targets. An

example of key terrain in the air domain could be an opening or divide in a mountainous region that allows for maneuverability of rotary wing aircraft to maneuver. As it is known that rotatory wing aircraft are not ideal for maneuverability through high elevations or urban environments therefore securing a more desired maneuver corridor that will allow for air assets to maneuver on the battlefield may be necessary. The airspace over an objective or target could additionally be considered key terrain.

4. Space Domain

Space is a continuous environment that is the most complex of the physical domains. The space domain has some unique characteristics that include: Orbital Mechanics, Environmental Considerations, Electromagnetic Spectrum (EMS) Dependency, and No Geographical Boundaries (USJCS, 2013b). The lack of boundaries make it difficult to marks borders or areas. Therefore, the physical elements that do reside in space present the most likely key terrain, such as satellites or space stations. The lack of geographical boundaries is a very similar characteristic that is shared with the cyber domain and it is notable that the space domain draws the closest comparison to cyberspace in term of challenges, complexity, and uniqueness.

F. KEY TERRAIN COMPARISON IN LEVELS OF WAR

Key terrain will vary within the levels of war demonstrating that it changes dependent on the operational level and perspective it is being viewed from. The three levels of war consist of the strategic, operational, and tactical levels (see Figure 3) (Department of the Army, 2008). Each level possesses different responsibilities in terms of planning; decisions made in one level will directly affect the other levels. The key difference between the levels of war is in regard to the operational scale in which the commander is tasked. Strategic-level commanders operate at the higher echelons and are directing national policy and theater level strategy using national resources. (Department of the Army, 2008). “Operational-level commanders typically orchestrate the activities of military and other governmental organizations across large areas, while tactical commanders focus primarily on employing combined arms within an area of operations” (Department of the Army, 2008, p. 6–1, 6–2). Key terrain also changes at each level and

reflects upon the objectives of the commander and the desired end state. Using the example of the 2003 Invasion of Iraq, the strategic key terrain objective was seen as the countries' capital Baghdad. Key terrain at the operational level of war could be control of an area or route in support of the major operation to seize the capital. Key terrain at the tactical level would be more specific, identifying a geographic or manmade feature that is decisive to mission accomplishment and ultimately operational and strategic success.

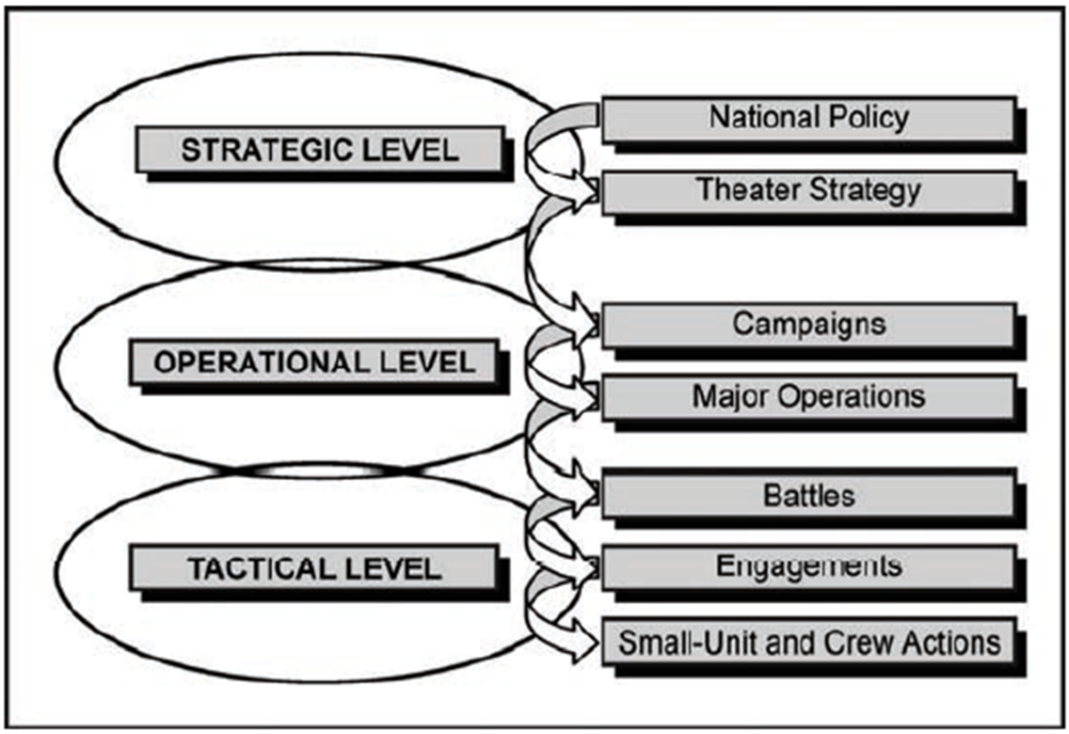

Figure 3. The Levels of War. Source: Department of the Army (2008, p. 6–2).

Addressing the levels of war is necessary as the concept of key terrain alters and varies between each level of war and must be examined in the correct context. This demonstrates how moldable the concept of key terrain becomes when applying it to different levels of war and draws similarities to that of cyberspace, in which actions can have implications and effects across multiple levels of war. Attention to the levels of war is drawn to determine if key terrain will have similar relevancy within the cyber domain.

G. CONCLUSION

From the military perspective, terrain must be analyzed and understood in order to leverage potential advantages on the battlefield. Terrain analysis is vital to military operational planning as it helps the commander understand the operational environment and identify key terrain. Key terrain is deemed important to the U.S. military for the pure fact that its possession can be the difference between victory and defeat on the battlefield. The teachings of Clausewitz along with lessons learned on the battlefield have shaped the importance of key terrain in U.S. military doctrine. In the Army, reference and use of the concept of key terrain starts with Troop Leading Procedures, at the lowest echelon of leadership (Company and Below). At this echelon, soldiers, from the company to the squad level, are exposed to the concept as they analyze the effects that terrain may have on the mission. This early exposure has resulted in a strong grasp of the concept in terms of the land domain.

This chapter outlined the foundational importance of the concept of key terrain. The focus thus far has been in the physical domains of land, air, and maritime. The next chapter transitions to the cyber domain, the focus of this thesis. With the foundational understanding of key terrain, it is evident that some critical points must be accounted for in the assessment of its applicability to cyberspace. These critical points include maintaining the correct operational context and ensuring that the terrain feature aligns with the doctrinal definition by providing an advantage to either side that controls it.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CYBERSPACE

A. INTRODUCTION

The emergence of cyberspace has drastically changed the daily lives of everyone in the world. Ideas once viewed as futuristic or impossible are now reality; with the ability to communicate and collaborate with people via electronic mail, transmit currency via the Internet, or view satellite imagery from anywhere in the world. These capabilities and many more are made possible due to cyberspace. Cyberspace is an environment that is purely man-made and consists of both physical and non-physical attributes. The environment of cyberspace offers challenges and complexities unseen in other warfighting domain and requires extra attention when applying the traditional concept of key terrain.

The DOD highly depends on cyberspace to support operations with heavy use of IT infrastructure and systems supporting intelligence, logistics, and command and control functions. This chapter specifically examines the question of what cyberspace is, and how it is important to the military. Answering this question along with outlining the unique characteristics of the cyber domain are necessary prior to application of key terrain.

B. WHAT IS CYBERSPACE?

> Cyberspace is the 'place' where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. *The place between* the phones. The indefinite place *out there*, where the two of you, two human beings, actually meet and communicate. (Sterling, 1992)

"Cyberspace is simply the manmade domain and information environment we create when we connect together all computers, wires, switches, routers, wireless devices, satellites, and other components that allow us to move large amounts of data at very fast speeds" (Williams, 2014, p. 14). All the interconnected devices and data that comprise cyberspace are manmade, from the IT infrastructure to the software, protocols, and resident data, all are created by man. The DOD defines cyberspace as an information environment "consisting of the interdependent networks of information technology

infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (USJCS, 2013a, p. I-1). This inherently means that cyberspace not only consists of end user systems and physical devices, but also the resident data as well as the interaction with this data that occurs in an abstract environment. This definition also presents the fact that the Internet is included as a comprising piece of cyberspace. The unique traits that distinguish cyberspace from other domains are its lack of physical characteristics, and its susceptibility to rapid changes that effectively alter its terrain or configuration.

1. Nonphysical Qualities of Cyberspace

Many of the objects and identities that exist within cyberspace are nonphysical, in that they lack any geospatial locations resulting in no ties to any physical location. In the land domain, fixed terrain features such as mountains, depressions, or valleys are tied to a geographic location. Cyberspace does not have this luxury. Instead the terrain includes objects such as "radio waves, cell phones, fiber optic cables, satellites, laser beams, software, firmware, and anything that can be linked together to create a network" (Magee, 2013, p. 77). The cyber terrain however does contain IT infrastructure, systems and communication mediums that exist in the physical domains but function in the cyberspace environment. These objects can be potentially fixed to one physical location but this is not guaranteed. These objects can be physically moved, reconfigured or logically altered in some way. The nonphysical characteristic of cyberspace is seen with the use of IP addresses. Addresses in the physical domain reference a physical location however, addressing in the context of IP addresses tells the user where to go, but it does not necessarily translate to its physical location.

2. Dynamic Environment

The element of human control and interaction in cyberspace allow for the environment to be highly malleable. Elements of cyberspace can be easily altered, added, or removed, resulting in constant changes to the topology of the terrain. These changes occur at profound speeds, which essentially means the landscape of cyberspace at this moment does not guarantee the same landscape the very next second. For example, minor

configuration changes to a wireless access point can have large implications on the overall layout of a network. If an access point with ten connected nodes is removed, the nodes become inaccessible changing the topology of the network. The human interaction with cyber identities such as email accounts, social media, and blogs also account for elements of cyberspace and are subject to change. This human interaction will result in the addition of data or the removal of data from cyberspace.

The fact that the environment of cyberspace is constantly growing and changing also results in a vast domain. After all, "cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them" (USJCS, 2013a, p. I-2). This demonstrates how large cyberspace is and continues to grow with various projections forecasting 30–50 billion devices to be connected to the Internet over the next 10 years. In addition, the rise of the Internet of Things (IOT) along with the transition to IPV6 support the fact that cyberspace is growing at an exponential rate and will continue to grow with no sign of slowing down.

C. CYBER TERRAIN COMPOSITION: THREE LAYERS

"The U.S. Army LANDCYBER White Paper 2018–2030," defines cyberspace terrain as the "Physical and non-physical terrain created by and/or composed of the human layer, logical layer, and physical layer" (U.S. Army Cyber Command, 2013, p. 46). JP 3–12 does not define cyberspace terrain anywhere in its publication but does describe a layered approach that decomposes cyberspace. Due to the unique terrain traits, it is understandable why many, including the DOD, divide cyberspace into multiple layers when discussing its terrain.

The DOD depicts cyberspace in three layers: physical network, logical network, and cyber-persona (USJCS, 2013a). Each of these layers represents a different grouping of objects and identities that reside in that specific layer.

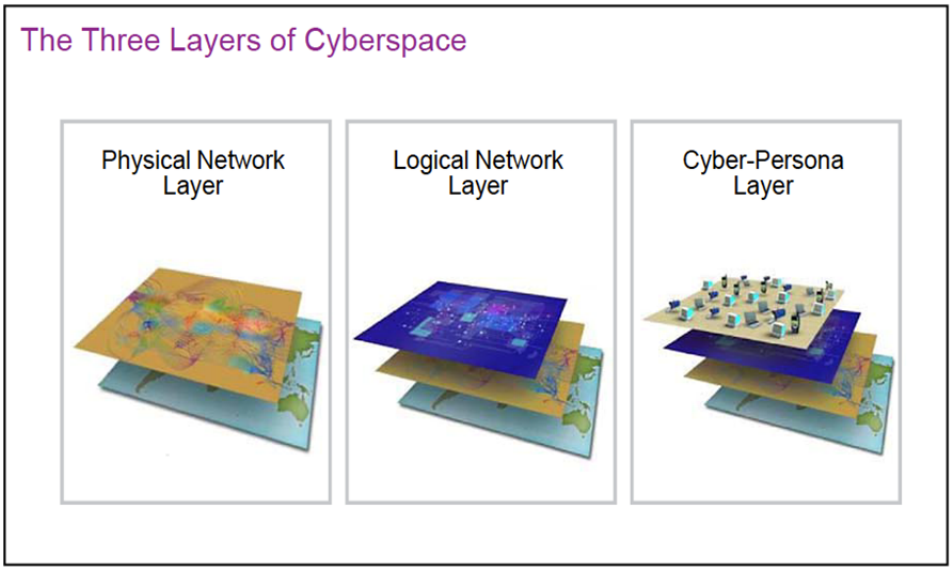

Figure 4. The Three Layers of Cyberspace. Source: USJCS (2013a, p. I-3).

The two components of the physical network layer include the geographic and physical network components. The geographic components are the physical location of the infrastructure, and systems that support cyberspace. They have the ability to not remain fixed in one location as discussed in the previous subsection. The physical network components are the media through which data travels and are "comprised of the hardware, systems software, and infrastructure (wired, wireless, cabled links, EMS links, satellite, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, switches, servers, and computers)" (USJCS, 2013a, p. I-3). The physical network layer shares a relationship with the physical domains in that its infrastructure and objects operate in their domains. The physical layer is the easiest to understand as it shares similarities to the terrain principles of physical domains.

The logical network layer is abstract in that it encompasses various elements such as software, operating systems, system data, and protocols all of which allow the exchange of information in cyberspace to be possible. These elements are related in an abstract manner from the physical layer but are not tied to an individual, specific path, or node (USJCS, 2013a). An example of this could be a website URL. The URL's address is used to route the user to a website's server. The URL identifies the website but it does not identify a physical location as the web servers may be located in multiple physical

locations. At this layer one can begin to see potential challenges to applying key terrain in cyberspace.

"The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. … However, one individual may have multiple cyber-persona, … [and a] single cyber-persona can have multiple users" (USJCS, 2013a, p. I-3, I-4). Digital representations include: email, social media, phone numbers, or web presences that can be tied to an individual or group. Cyber personas are a common trend among people all over the world with approximately 2.3 billion social media users active today. Using Facebook as an example, it is possible for one user to create multiple user accounts or link their account to other social media accounts and emails, resulting in multiple cyber personas. Additionally, users may share a cyber persona, as is seen with social media accounts for organizations in which multiple people access the same account, sharing information and data. Cyber personas can also include administrative level accounts on a system or network, which serve as high value targets to opposing forces. The cyber persona layer is abstract and complex in the fact that elements will reside in many virtualized locations and will rarely be linked to a centralized location. This again demonstrates a potential challenge for key terrain application in the cyber domain.

D. DOD AND CYBERSPACE

The Internet is the most notable network that resides in cyberspace. Many may simply define cyberspace as the Internet or vice versa, but the Internet is just one entity of cyberspace. The Internet originates back to the 1960s when the U.S. Government commissioned research to develop computer networks in order to share information between various military research facilities. The research gained the interest of academia intrigued with the idea of sharing data and information with fellow universities. The progression in research resulted in the development of the Advanced Research Projects Agency Network (ARPANET), which was an early packet switching network and the first network to use the TCP/IP protocol ("Internet," n.d.). This introduced the ability for

networks to connect to other networks, allowing one location to exchange and share information with another physical location. With continued research, funding, and advances in technology, the Internet is now a global system of interconnected computer networks that link a wide variety of devices together ("Internet," n.d.). Some of these devices include computers, mobile phones, and tablets, but more recently everyday objects such as thermostats, refrigerators, televisions, and automobiles are becoming connected devices, making up the "Internet of Things." Governments, banks, and societies all over the world now rely on the functions and capabilities that the Internet provides, thus solidifying the importance that cyberspace holds today.

The reliance and importance of cyberspace is no different for the U.S. military. Cyberspace benefits the DOD in many ways and now has become fully integrated into almost every aspect of the military. The DOD's original requirements to simply share data between research facilities and installations has dramatically expanded. The military is now heavily dependent on cyberspace to conduct day-to-day operations and support warfighting functions. The DOD relies on cyberspace to enable functions such as logistics, global command and control of forces, intelligence, and remote operations (Lynn, 2010). Common everyday functions such as electronic mail and telecommunications are the most notable cyberspace uses of the military, but systems such as the Army's Standard Army Maintenance System—Enhanced (SAMS-E) and the Blue Force Tracker (BFT) are examples of technologies that are now viewed as essential to those that use them.

SAMS-E allows for the U.S. Army to order and track over 1 million vehicle and repair parts in an expedited manner permitting high levels of readiness (McLane Advanced Technologies, n.d.). It is now a common fixture within Army units with commanders relying on it to maintain unit readiness and effectiveness. The BFT is an example of a command and control or mission command system that is heavily relied on by ground forces providing real-time location updates using GPS, instant messaging, and IP-capable networking to mobile air and ground platforms (ViaSat, n.d.). Recent conflicts in Afghanistan and Iraq have demonstrated the benefits that the BFT provides the warfighter by allowing units real-time tracking of friendly forces, movements, and

additional contingency communication capabilities all from an embedded console in their vehicle.

Both technologies are extremely beneficial to the warfighter and it is important to note that the supporting infrastructure and data that allow for its functionality resides in cyberspace. These systems network with other systems and databases in order to communicate needed supplies or communicate positioning of Soldiers on the ground. While the infrastructure may physically reside in another domain (land, air, maritime, or space), it all functions and interacts in cyberspace. Cyberspace allows for efficiency in the military as tasks are now able to be completed in quicker periods of time. The DOD has pushed for "net-centric operations based on digital communications and ease of access to information at all levels, down to the individual soldier on the battlefield" (Arquilla & Goldman, 2014). This benefit along with the ultimate ability to communicate makes cyberspace instrumental to the success of the U.S. military. With the use of cyberspace and its benefits come threats and vulnerabilities.

1. Emergence of Cyber Warfighting Domain

With the great benefits cyberspace offers to the military there are also risks and threats to its functionality, which have great implications on military operations. Like other warfighting domains, cyberspace is not free of malicious actors with the intent of taking advantage of vulnerabilities or do harm. Nation states, hacktivist, and script kiddies are at the forefront of attacks in cyberspace and the DOD's presence in cyberspace is a highly sought after target. Between September 2014 and June 2015, the DOD acknowledged that it had endured 30 million malicious intrusions on DOD networks (Department of Defense [Memorandum], 2015). While only a small percentage were actually successful, these threats and vulnerabilities now require defensive measures in order to protect people, data, and IT infrastructure from the risk of physical, economic, or media damage.

The potential for cyberspace to be used with the intent to destroy, disrupt, deny, or degrade an enemy's resources or operations demonstrated the potential for a new form of warfare. This realization, along with the need to secure critical data and infrastructure

fueled the efforts that eventually allowed cyberspace to be recognized as a domain. To better scale efforts to protect DOD in cyberspace, then Defense Secretary Robert Gates ordered the consolidation of task forces into a newly formed U.S. Cyber Command (Lynn, 2010). Led by a four-star commander, they would begin operations in May 2010 as a sub unified command of U.S. Strategic Command (Lynn, 2010).

Recognizing that cyberspace possesses the attributes of a space in which warfare could occur, the DOD recognized the cyber domain. This independent domain only marginally resembles the other domains, as the cyber domain introduces an environment filled with non-physical attributes, logical data, and user personas. The terrain of the cyber domain challenges current doctrine, processes, and strategies of warfare. Retired General Keith B. Alexander reiterated this point stating, "While the time-tested principles of war will ultimately apply in cyberspace, its characteristics are so radically different that they demand significant innovation and changes to the way we organize and conduct military operations and tactics in this domain" (Alexander, 2007, p. 59).

2. DOD Cyberspace Operations

The DOD defines cyberspace operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (USJCS, 2013a, p. II-1). Cyberspace operations are "those conducted in cyberspace with the objective of providing friendly freedom of maneuver in cyberspace and projecting power in and through the domain in support of JFC campaign objectives" (Williams, 2014, p. 14). Cyberspace operations are categorized by their intent and are identified as offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), or DOD Information Network operations (DODIN-Ops).

Offensive cyberspace operations are operations in which the intent is "to project power by the application of force in and through cyberspace" (USJCS, 2013a, p. II-2). Defensive cyberspace operations are operations in which the intent is "to defend DOD or other friendly cyberspace" using active and passive cyberspace operational measures (USJCS, 2013a, II-2). DCO is important as it is most likely occurring inside a friendly network and includes activities such as hardening of systems and hunting for threats.

"DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation" (USJCS, 2013a, II-3). DODIN-ops support and protect the vast needs and daily operational services that the DOD is reliant on. This includes IT platforms, service and agency networks, industrial control systems, mobile devices, and tactical communication systems that all support the DOD (Daniel, 2016).

Cyberspace operations provide freedom of movement through cyberspace, they can deny the enemy freedom of maneuver, and can explicitly support campaign or mission objectives. They have purpose and are executed with careful planning similar to that of the other domains. Understanding the operational environment still applies in cyberspace and IPB is still conducted to help understand the terrain, which includes identification of key terrain.

E. COMPARISON OF CYBERSPACE TO OTHER DOMAINS

When comparing the cyber domain to the other domains there are some noticeable observations. First, cyberspace is dependent on other domains to operate and has certain interdependencies with specific domains. Second, the cyber domain is borderless. Last, maneuverability within the domain is unlike that in any of the other domains. Discussion of these key points along with others will draw the similarities and differences between the domains. This is imperative to gaining insight into potential challenges or similarities cyber has to other domains when trying to apply the concept of key terrain.

1. Cyber Dependencies

Understanding the cyber terrain alerts us to the unique relationships and differences the cyber domain shares with the land, air, maritime, and space domains. Cyberspace relies on the fact that the physical devices, nodes, and infrastructure that support it, all reside in the other warfighting domains. Examples range from satellites in space, underwater cables in the ocean providing a backbone for communication between nations, or antennas on top of buildings, all of which exist in other domains but function in the cyber domain. This is seen with the unique relationship between space and

cyberspace in that "virtually all space operations are dependent on cyberspace, and a critical portion of cyberspace can only be provided via space operations" (USJCS, 2013a, p. I-2).

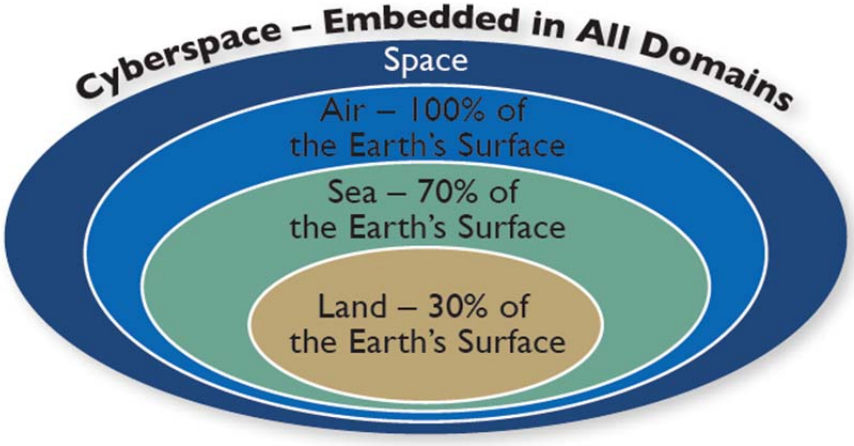

Figure 5. Domain Interaction. Source: Welsh (2011, p. 3).

Welch's figure shown in Figure 5 demonstrates how cyberspace is embedded into all the other domains. Cyberspace must interact and is highly dependent on each domain to function. "Military operations in all domains depend on operations in, through, and from cyberspace" (Welsh, 2011, p. 3).

2. Borderless Environment

Cyberspace has no definitive borders like the other domains. The transactions, and data exchanges occur within cyberspace and circulate through devices such as routers and servers all over the globe. Identifying ownership of cyberspace is impossible purely on the basis of its composition and functionality. As discussed earlier, there are no physical ties to locations making the ability to map areas of responsibility or ownership difficult. "The ubiquitous nature of cyberspace creates another major consideration in CO [cyber operations], because it enables an adversary to establish key points of presence outside the physical operating area" (USJCS, 2013a, p. II-10). This ultimately means that there is no definitive battlespace or area of operations in cyberspace. Cyber operations are

not restricted to one particular area and an enemy can attack from anywhere, which is unseen in any of the other domains.

However, there is some similarity between cyberspace and space when it comes to borders. Neither has definitive borders that can be drawn and enforced. The maritime domain also presents some challenges in this sense, but agreements among nations have politically determined borders that outline national and international waters. Cyberspace however does not allow for lines to be drawn in the sand making the identification of friendly cyberspace versus non-friendly cyberspace impossible.

3. Maneuverability in Cyberspace

The cyber domain's malleable environment affects maneuverability within the cyber domain. When the stage is set for a battle in the land domain an area will be selected for engagement and the means of getting to that area will be planned. This is not the case in the cyber domain. There is no set area for engagement and the route to a target can change in the blink of an eye as the enemy has the potential to change the configuration of the battlefield at any time, making maneuverability a challenge.

In addition, like other domains maneuverability during military operations must account for legality, sovereignty, and political considerations. However, the lack of definition or agreement on these considerations in cyberspace equates to greater challenges when addressing these topics. Legalities of warfare in the cyber domain remain in development and there is a large disparity among nations on how these should be addressed. The *Tallinn Manual* is working toward the discussion and establishment of such legalities but still requires worldwide acceptance. Sovereignty is challenged by the borderless environment possessed by cyberspace in which data circulates through routers, switches, and servers that are housed in various physical locations and physical devices. Sovereignty and ownership of cyberspace exudes the issue of attribution in cyberspace. Determining threats and identifying those responsible for attacks in cyberspace presents another difference within the cyber domain. Within cyberspace, attacks require more forensics and intelligence to attribute their true source. Adversaries in cyberspace are afforded abilities, unseen in the physical domains, to obscure their identity. These

challenges demonstrate more of the key functional differences that the cyber domain presents.

F. CONCLUSION

The cyber domain is vital as it houses all the technologies and systems that the military relies on to function. It has emerged as a warfighting domain and the application of military strategies and tactics is required to support cyberspace operations. There are considerations that have been derived from this chapter that must be accounted for when analyzing key terrain's application in cyberspace. These considerations include the nonphysical characteristics of cyberspace, the dynamic environment of cyberspace, and the absence of borders, which influence maneuverability. Lastly, we discover that cyberspace is dependent on other domains for functionality, which could potentially mean that key terrain could exist in other domains but directly affect the cyber domain. An additional set of considerations that must be tested is the three-layer composition of cyberspace. This unique terrain composition must be tested against the concept of key terrain to understand how the concept relates at each layer. These considerations can potentially influence where key terrain resides in cyberspace and how it can be found.

IV. KEY TERRAIN AND CYBERSPACE

A. INTRODUCTION

Outlining the importance of the concept of key terrain and the emergence of the cyber domain allows for an assessment of if or how the concept of key terrain fits in cyberspace. Prior to making this assessment correct terms and contexts must be applied by clarifying what is not key terrain. Walking the concept through each layer of cyberspace, including all considerations, while using correct terminology and contexts should allow for an answer to the research question posed by this thesis. Additionally, the considerations outlined in the previous chapter must be represented in order to determine if they influence the application of key terrain. This chapter concludes with that assessment on whether the unique challenges and layers of cyberspace require a cyber-specific definition.

B. WHAT CYBER KEY TERRAIN IS NOT

There are other military and private sector vocabulary terms that bear similarities to the concept of key terrain but are inherently different. The definitions of these terms share some similarities to key terrain but they differ in the context of operations. Examining these terms filters out the misconceptions that interfere with key terrain's application to cyberspace. These terms are not the same as key terrain:

- Crown Jewels—"a process for identifying those cyber assets that are most critical to the accomplishment of an organization's mission" (MITRE, n.d., para. 1 (definition)).
- Critical Asset - "A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively" (USJCS, 2010, p. 55).
- Critical Infrastructure - "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (U.S. Patriot Act of 2001).

Crown jewels analysis or CJA accounts for the fact that not every cyber asset can be configured and designed to withstand any APT. Instead CJA identifies mission critical assets ensuring that those cyber dependent assets are designed and configured to withstand APTs. Using this type of analysis can scope a large network down to a smaller group of assets in which resources and additional security efforts can be placed. This type of analysis fits in the context of risk management or threat modeling, where critical assets need to be identified and protected, but differs from key terrain in a few aspects. In cyberspace, key terrain looks for objects in the layers of cyberspace that would afford an advantage if seized. CJA is looking for cyber assets that are critical to mission accomplishment and the organization's ability to operate. CJA is strictly from a defender point of view and is purely focused on looking at the cyber assets internal to the defender. While penetration testers take an attacker perspective it is still not in the same context as a military cyber operation.

Critical assets focus on entities that if lost would severely hurt the nations' ability to function. This is an internal organizational view to identifying critical assets owned by the organization or unit. These assets are prioritized into a list called a "critical asset list" which the DOD defines as "a prioritized list of assets or areas, normally identified by phase of the operation and approved by the joint force commander, that should be defended against air and missile threats" (USJCS, 2010, p. 55). The "critical asset list" prioritizes the critical assets while the "defended asset list" prioritizes the defense of these assets with the resources available (USJCS, 2010). Key terrain maintains a more offensive and defensive operational context while critical assets focuses more on the overall operation. Critical assets are viewed mostly as internal assets that are critical and must be defended in order to sustain the nation's ability to function.

Another common misconception is that critical infrastructure and key terrain are the same. With the prevalence of IT systems and architecture dominating the operational functions of critical services and needs, it is understandable how one could mislabel the two. Careful differentiation must be placed between critical infrastructure and key terrain, as they are not the same. Like critical assets, critical infrastructure is examined from a more defensive posture. Critical infrastructure is seen as vital to the U.S. livelihood.

Analysis to find critical infrastructure is done as a preemptive effort to identify systems and assets to harden and protect. Conversely, key terrain is looking for similar assets but with the intention of exploitation or protection in a military cyberspace operation. There is the potential for certain cyber critical infrastructures to be identified as key terrain if it pertained to a cyber operation and afforded an advantage to that operation. However, critical infrastructure is very broad and its association to national security and livelihood imply that it is a target to be cautious of as it has great ramifications. It is understandable to identify a power station as critical infrastructure but to label it as cyber key terrain is too broad. Key terrain in cyberspace is more specific, and would need to identify a specific cyber entity that fit in the cyberspace layers. For example, rather than the power station, cyber key terrain could be a SCADA network entry point. This is very similar to the "sensor to shooter" concept in which analysis must be conducted to find the specific points of entry and vulnerabilities to exploit. Thus, critical infrastructure is important to identify and protect but differs from the concept of key terrain.

There are definitional similarities between CJA, critical assets and critical infrastructure which undoubtedly causes some to use them interchangeably. It is not uncommon for companies and organizations in the private sector to use or adapt military terminology but key terrain is only identified and applied to military operations. The private sector is focused on cyber security and defensive activities to protect the assets that are vital to their organizations and are not conducting offensive and defensive cyber operations like the DOD. Establishing this clear difference does not negate the usefulness of these terms in cyberspace and is more focused on ensuring the correct terminology is used when applying key terrain to cyberspace.

C. APPLYING KEY TERRAIN TO THE LAYERS OF CYBERSPACE

As discussed in the previous chapter the DOD divides cyberspace into three layers. There may be certain layers in cyberspace where key terrain applies better than others. Understanding the layers and what key terrain elements exist will ultimately determine if the concept adapts to cyberspace. When examining each layer the perspective of a military cyber operation must be maintained in order to keep the correct

context. The following discussion examines considerations for key terrain at each layer, examples of what key terrain might be identified at that layer, where it breaks down, and what changes to the application of key terrain may be required.

1. Key Terrain at the Physical Layer

Applying the concept of key terrain to the physical network layer aligns with the concept's traditional use. This is because elements at the physical layer exist in the other physical domains and can potentially be tied to a geographic location, though some have the ability to move or change. This layer includes the geographic and physical network components necessary for networks to function. Geographic components physically reside in the land, maritime, air, and space domains. Physical components such as the infrastructure, computers, and wiring also reside in the physical domains. This is the only layer in which humans can physically interact with components. For example, a wire can be unplugged or a router physically moved.

Applying key terrain at the physical network layer requires analysis of physical and geographic components in an area of operation. This analysis will yield a map of certain cyber terrain elements that are of advantage to whomever controls them. For example, key terrain at the physical layer could be a vulnerable wireless medium that controls traffic infrastructure in an area of operation. While conducting a study, a group of researchers was able to access the wireless communication of a traffic system's network through vulnerabilities in encryption, and use of default usernames and passwords (Ghena, Beyer, Hillaker, Pevarnek, Halderman, 2014). This could be identified as key terrain if the intent was to cause a disruption or alter the traveling path of a moving target. The poor security posture of a physical wireless medium is an example of using a physical network layer object as key terrain.

Another physical layer key terrain example is the actual physical wires and cables carrying data across a nation. In September of 2015, the FBI investigated the severing of two AT&T fiber-optic cables that supported a large spoke of area communications infrastructure in San Francisco, California (Howell, 2015). The high-capacity lines carry vast amounts of data including voice communications and computer transactions making

them appealing key terrain targets (Howell, 2015). This specific incident disrupted seven 911 call centers (Chu, 2016). These cables span the globe, including traversing the oceans. In the maritime domain, most underwater sea cables are cut within a few miles of shore and are easy to repair but cutting cables at further depths out in the middle of the ocean could potentially cripple communications for some time (Sanger, Schmitt, 2015). This demonstrates that even a specific portion of cable could be considered key terrain based on the advantage it would provide.

The concept of key terrain has the potential to break down at this level because of the ability for physical layer elements to move. Some objects at this layer will be fixed to a geographic location but most will not due to their mobility and their ability to be physically configured or moved by humans, as presented in the example of the cut fiber lines. The mobility of objects at the physical layer presents a challenge when identifying key terrain as it could exist at one moment and gone the next. This will require additional care when identifying physical layer elements as key terrain. Key terrain at this layer can be identified by mapping and understanding physical infrastructure and mediums of a network. Persistent monitoring methods will have to be introduced into the planning processes of military operations to ensure geographic and physical components of this layer have not moved.

2. Key Terrain at the Logical Layer

The logical network layer of cyberspace introduces the first of the non-physical layers. The objects in this layer have no geographical location and are not necessarily tied to a specific node. The logical layer is everything between the communication mediums and systems of the physical layer. Interactions at the logical layer include protocols telling packets of data where to go, the machine code telling a computer how to process data, and the DNS server resolving web addresses to their respective IP addresses.

Applying the concept of key terrain to the logical layer requires more thought than is required of physical terrain. Key terrain at this level could be a logical port in which control is necessary to launch exploits or tools. Control of a port could be relatable to controlling a bridge in the physical domain. Control allows for monitoring or the

ability to stop network traffic into and out of that logical port. Logical ports associate IP addresses and protocols and as the name implies they themselves are logical and have no physical presence or location.

The 2008 Russian Georgian War provides an example, indicating likely identification of key terrain in order to achieve cyber effects. This war was the first time a conflict witnessed cyberspace being used in synchronization for combat actions with other warfighting domains (Hollis, 2011). The Russians launched a series of DDoS attacks on Georgian networks denying communications and simultaneously conducted information exfiltration activities to collect intelligence (Hollis, 2011). website and hacker forum defacement was conducted for propaganda and counter-attack mitigation measures (Hollis, 2011). These actions demonstrate that the Russians most likely identified certain cyber features as key terrain, in this case websites and forums. They gained access to these sites by exploiting poor security measures, possibly through SQL code injection or cross-site scripting attacks, and denied access and altered data. In order to deny access to websites using DDoS attacks, the Russians would need to identify ports and IP addresses (logical layer elements) as key terrain due to their control being necessary to facilitate the desired effects. This historical example does not explicitly label key terrain but it does imply that the Russians had selected specific cyber terrain that would support their operations.

Key terrain at the logical layer can potentially break down due to the care that must be placed in its identification. Identification of key terrain at the logical layer will require enumeration and scanning of the area of operations in cyberspace. This provides vital intelligence needed to map the nonphysical network such as information on operating systems, configurations, and logical addresses. There is the potential for logical layer terrain to change, which hinders the ability to capture an accurate depiction of the layer. As discussed in Chapter 3, terrain in the logical layers can be reconfigured and change moment to moment. This will again require continued monitoring throughout the operational planning process in order to ensure the key terrain still exists. An additional challenge is how to define control in the logical layer. Applying a concept like key terrain would imply that the retention and control of a logical layer element would allow an

advantage during operations. However, the ability to actually control or retain a logical layer element could be considered unmeasurable. If you mount forces on a hill they can generate an assessment of its control by visual observation. In cyberspace and specifically the logical layer this assessment is not as easy to measure. Logical layer elements can have multiple users at one time with neither realizing they are there.

3. Key Terrain at the Cyber-persona Layer

The cyber-persona layer is another non-physical layer and encompasses the cyber identities that most notably include email accounts, administrator accounts, and social media accounts. Possession of these accounts would yield great advantage to whomever controlled it and could be identified as key terrain should its control be necessary to achieve an operational outcome. Therefore, key terrain at the cyber persona layer will often be user accounts.

In January 2015, hackers claiming loyalty to the Islamic State of Iraq and Syria (ISIS) compromised Twitter and YouTube accounts owned by USCENTCOM. Twitter, a popular social media service and YouTube, a site that hosts user video content, were both used by USCENTCOM as effective communication tools for the media, service members, and families. The hackers defaced the Twitter account by adding messages such as “American soldiers, we are coming, watch your back. ISIS.” and “We broke into your networks and personal devices and know everything about you. You’ll see no mercy infidels. ISIS is already here, we are in your PCs, in each military base” (ZeroFOX, 2015, para. 2–3). The hackers then claimed to have obtained “classified” information from these accounts and threatened to disseminate various PII to include names, phone numbers, an email addresses of military personnel. (ZeroFOX, 2015). The compromise of these accounts was short lived but their ability to gain access and control of USCENTCOM’s social media accounts demonstrated a cyber persona layer key terrain from an enemy’s standpoint. The act was labeled cyber vandalism but it did allow the enemy to alter messages of a combatant command which could have potentially degraded the mission, hurt morale, or compromised sensitive data housed on these sites.

Key terrain at the cyber persona layer can potentially break down for two reasons. First, accounts can change and adversaries can hold many accounts. This requires the careful monitoring that is necessary of the previous two layers. Second, there remains an issue with the term "control." How one would control a cyber persona is hard to judge. For example, users may not notice that their email account is compromised until they see unfamiliar messages in their sent items outbox. However, the cyber persona can be seized, and does not degrade its usefulness as long as the realization is made while applying key terrain at this layer. Contingency key terrain should be selected due to the volatility of the terrain at this layer.

A concluding point that applies to all the layers is the fact that key terrain identification will vary based on who is looking at it. The application of key terrain in the cyberspace layers is necessarily subjective, although it should not be arbitrary. Two commanders can look at the same operation and based on the current state of the environment and the intelligence on hand, select two different cyber key terrains. It is not unfathomable for someone to look at each of the examples and identify different points of access or cyber identities that would meet the definition of key terrain for the given context of a mission or operation. Therefore, careful attention must be given to utilizing the concept of key terrain in cyberspace, especially when applying it to non-physical layers, as these tend to be the most volatile and abstract. Based on this assessment and the nonphysical layers of cyberspace one may question if there is indeed a need for cyber specific terminology to define concepts like key terrain in cyberspace.

D. IS A DOCTRINAL CYBER-SPECIFIC KEY TERRAIN DEFINITION NEEDED?

As acknowledged in the literature review, there is currently no definition for cyber key terrain in military doctrine. JP 3–12 references cyber key terrain when discussing movement and maneuver, stating that the concept of key terrain is essential to planning. The DOD uses one standard definition for key terrain when defining it throughout all domains as found in each service's doctrinal publications. Focusing on the cyber domain, JP 3–12 presents some broad examples of what objects or features in cyberspace may be identified as key terrain to include, "…major lines of

communications; key access points for the defense, observation, and launch points for the offense; or opportunities to create bottlenecks" (USJCS, 2013a, II-10). This is a broad overview of potential cyber terrain features, but does not serve as a definition that can be used to define cyber key terrain. At first glance the absence of a cyber key terrain definition may appear to be an oversight or flaw in doctrine. This however may not be the case as there are no other domains with a specific key terrain definition. The concept's application should not be hindered by the absence of a doctrinal cyber-specific definition nor should it cause confusion. There are three reasons why a cyber-specific key terrain definition is not needed.

First, based on the organic and constantly changing environment of cyberspace, no clear cyber key terrain definition can be given, because what would apply today does not apply tomorrow. The steady advancement of technology additionally affects the terrain of cyberspace. This unstable terrain creates a moving target that is hard to place a fixed definition on. The volatility of key terrain at each of the layers of cyberspace additionally demonstrates this problem.

Second, doctrinal strategies and processes are already in place. Efforts to build a cyber-specific definition for a concept that would equate or mean the same thing as key terrain would not be valuable. Understanding the operational environment is a requirement in military planning regardless of the domain and the use of traditional military concepts such as key terrain help to alleviate misunderstandings. Applying the concept to cyberspace generates specific viewpoints that military leaders regardless of their background can understand. Using the term "key terrain" is productive in the fact that it is understood in the military vocabulary and would ensure commanders are involved and interested in the cyber planning (Williams, 2014). Maintaining a common understanding is essential to effectiveness of integrating combatant commands and cyber assets for operational planning.

Third, other domains do not establish domain specific definitions for key terrain, but do provide examples of what potential key terrain features would apply to their environments. Their examples demonstrate some of the unique features that can provide key terrain advantages in their domains, but do not alter the foundational concept of key

terrain. This observation leads one to believe that the doctrinal definition of key terrain already has the flexibility to be molded to the operation and the domain as long as it follows the guiding principles of the concept.

The layers of cyberspace do challenge the definition but do not point to the necessity of creating a term. It is easy to see both sides of the argument but there is great value to maintaining a term that is used to describe a long-standing military strategy. There is no evidence exemplifying the value that would be added by developing a domain-specific definition for key terrain. The challenge to its application does not inherently lie in the absence of a doctrinal definition for the domain, but more in the understanding of the cyber terrain. Therefore, use of the traditional key terrain definition will suffice in cyberspace.

E. CONCLUSION

The general concept of key terrain is defined as "Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant" (USJCS, 2009, II-13). When examining the terrain at each of the layers of cyberspace, there are inarguably certain terrain features that the seizure or retention of which will afford an advantage. Despite the complexity of the cyber domain the principal concept remains the same, only key terrain "involves network links and nodes that are essential to a particular friendly or adversary capability" (USJCS, 2013a, II-10). "Any area or locality" can encompass key points of access, social media accounts, or physical wires. Seizure of these may be identified as key terrain and essential in a defensive or offensive cyber operation. An operation to suppress an enemy's information operation campaign may determine a web address or social media account used to distribute propaganda as key terrain due to the advantages of its seizure and retention.

The absence of a cyber-specific key terrain definition does not distract from its application to cyberspace. When taking the concept of key terrain at its definitional root and applying it to cyberspace, it appears to have value. When disregarding the complexities and abstraction of cyberspace it is even clearer that the concept of key terrain applies to the cyber domain. However, the non-physical layers of cyberspace do

present the largest challenge to the concept's applicability in cyberspace. The characteristics of cyberspace terrain will have to be continuously monitored and mapped to ensure effectiveness of key terrain identification. The challenges do not remove its applicability, they simply require the need for additional care when identifying cyber key terrain. However, despite all this, the concept offers benefits or utility and should be maintained as a distinct term, not to be confused or replaced with the other cyber concepts.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. OVERALL EVALUATION

This thesis determines that the concept of key terrain can apply to the three layers of cyberspace. Its application is done so in a similar manner as the other domains. The previous chapter concludes that cyber key terrain identification takes more thought, must account for additional considerations, and is not clear cut. Key terrain in cyberspace is also not as easy to visualize like other domains. However, these challenges do not take away from the fact that the concept of key terrain applies and holds value in the context of military cyberspace operations.

In answering the research question this thesis discovers important considerations that influence the application of key terrain in cyberspace. These considerations are summarized here:

- Key terrain requires constant reassessment of the cyber terrain due its dynamic nature.
- Seizure and retention of key terrain can be difficult to measure.
- Key terrain only exists under certain conditions, therefore context matters.
- Understanding cyber key terrain is an art, not a science.
- A cyber key terrain definition is not necessary but methods of application would be helpful.
- Future doctrine, education and training is necessary in order to ensure that military tactics, strategies, and concepts such as key terrain are properly adapted in cyberspace.

Chapter III presents the point that unlike the physical domains where terrain features remain fixed and geo-located, terrain in cyberspace allows for unpredictable changes to its terrain. This volatile terrain requires constant reassessment and analysis of the operational environment in which a mission will transpire. Identification of key terrain in cyberspace will require continual monitoring and evaluation as it could disappear or a more advantageous terrain feature could appear. The traits of cyber terrain will require some additional processes to current doctrine and planning as terrain analysis within the

cyber domain must occur continuously and often throughout the cyber planning process. Network mapping, scanning, and enumeration will play a large role in cyber terrain analysis, maintaining current snapshots of the cyber terrain. This consideration has great implications on how and where key terrain will be found.

Chapter IV presents the fact that retention and seizure of terrain in cyberspace can be challenging to measure. Cyberspace's malleable terrain allows the potential for multiple individuals to interact or maneuver with or through an object. This is done sometimes without opposing parties knowing the others are even there. There are also techniques such as use of rootkits that cloak or conceal access and activity from users or administrators. This can potentially make assessing the seizure or retention of key terrain difficult and should be a consideration when identifying key terrain. Choosing cyber terrain that can be controlled effectively or in a measurable way should be considered during planning. Monitoring tools and techniques will help assess the seizure and retention of a non-physical cyber terrain feature but could be flawed.

Key terrain can only exist under certain conditions as presented in Chapter 2. Clarification between key terrain and other terms were established in Chapter 4. Careful consideration must be taken to ensure that the identification of key terrain and the use of its terminology are done in the correct context. The two needed components necessary to use the concept of key terrain in cyberspace are an operation (OCO, DCO, or DODIN-Ops) and an adversary (someone to apply the effect upon). If either of these two components are missing, the application of key terrain lacks the foundational principles set forth by military doctrine. The context must meet the correct conditions before key terrain becomes identifiable.

Another consideration is that the identification of key terrain is an art more than a science. Every commander will identify key terrain based on the intelligence, counsel of staff, and understanding of the operational environment. Key terrain is not black and white in cyberspace, and it is important to note that it is not always so in the other domains. Cyberspace's unique characteristics and an individual's technical skills, analytical skills, and overall creativity will result in variances in key terrain identification. Differing choices

are not necessarily wrong. This does not discredit the identification of key terrain but planners must understand that there may not be definitive answers as to what is key terrain.

Chapter IV concludes with the assessment that a cyber-specific key terrain definition adds no value. Despite the varying environments of the warfighting domains, they do not specify domain specific key terrain definitions. The cyber domain is no different and relies on the traditional definition of key terrain in its doctrine. The belief is that the concept of key terrain is clearly defined in military doctrine and it is worded in such a way that it can be shaped to fit into any domain regardless of how malleable or complex it is. Military leaders already understand the concept in the physical domains and the creation of a separate definition only further segregates cyber from other domains. Maintaining the concept's use in cyberspace will ensure that everyone understands what is cyber key terrain.

The final consideration is made based on the overall assessment of this thesis. Clarity is needed in DOD's cyber doctrine when discussing key terrain. Simply giving examples is not enough as there is not a one size fits all list of examples of cyber key terrain. Examples tend to be physical network layer devices and do not focus on non-physical key terrain. Even more complicating is the issue that the DOD does not define the terrain of cyberspace as has been done with other domains (Raymond, Conti, Cross, 2014). More focus on defining cyber terrain will result in a better understanding of key terrain. Cyber warriors must study the basic concept of key terrain not only to ensure they have an understanding of the concept but also to effectively apply it to the cyber domain. Engraining the concept into the minds of the cyber work force similarly to that of ground fighting soldiers will ensure that the necessary analysis is taken and that the concept is properly executed in the cyber domain. Understanding of the concept of key terrain is engrained in officers in the Army through the Troop Leading Procedures at the company level and below and through the military decision making process for Battalion and higher echelons. The understanding of this concept is necessary for cyber warriors to defend this domain. Education of these warriors on the traditional concept of key terrain is essential to achieving cyber dominance. These cyber warriors are the future leaders and will be able to in turn educate and teach current commanders on the concept of key terrain in cyberspace.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

This thesis focused on determining if the concept of key terrain applied and if so held value in the cyber domain. This served as only a starting point to the potential of works that can progress and enhance understanding of the adaptation of military doctrine, strategy and tactics to cyberspace. This thesis exposed certain areas of study that would progress the development of cyber doctrine and the concept of key terrain in cyberspace. The recommendations focus on how to identify cyber key terrain, as it is a noted deficiency in the overall evaluation. The following are recommendations for future work and research that will further develop this topic:

- Test current terrain analysis frameworks and tools to determine their effectiveness in identifying cyber key terrain.
- Determine whether additional cyber domain doctrine will help to integrate military strategies like key terrain more effectively.
- Identify changes DOD should make to institutional training, if any, in order to preserve military tactics, concepts, and strategies for future cyber warriors.

Identifying a framework or tool that best assists in the identification of key terrain in cyberspace would prove beneficial and is an area of study that not many have attempted. The last two recommendations are focused on doctrine and training. Doctrine development within the cyber domain remains in the early stages and exploration into better integrating military strategies could prove beneficial to those working to develop relevant and effective doctrine on the subject. The final recommendation focuses on what the necessary changes, if any, the DOD should make to training cyber warriors on tactics and strategies in the cyber domain. All of these recommendations are in support of a better understanding within the cyber domain.

C. CONCLUSION

This thesis outlined the importance of the concept of key terrain in cyber warfare and more specifically its importance to the U.S. military. The importance of the concept of key terrain has been taught by many great military strategists who helped shape DOD doctrine. Military strategy and tactics in cyberspace remain in the early stages of

development, but the foundational principles and doctrine used in the physical domains are key to providing the direction for strategy implementation. When taking the concept of key terrain and applying it to cyberspace, there are notable uses and benefits to its application. Looking at the topology of a network, there will always be certain cyber elements that, when controlled, will allow for an advantage to friendly maneuverability or halting of enemy maneuverability. The instincts to challenge the concept's applicability in cyberspace are more likely rooted in unfamiliarity or misunderstanding of the cyber domain. Cyber operations warrant the same planning responsibilities as in any other domain and the identification of key terrain is no different.

This thesis only scratches the surface on the overarching challenge of adapting military doctrine to the cyber domain. Stating that it is a challenge may be an understatement. The real issue lies in a better understanding of doctrine and concepts prior to applying them to the cyber domain. Continuing to use buzz words or popular military terms without true understanding of their meaning can lead to misconceptions. This recommendation is only the beginning of an effort to question and challenge whether the traditional military tactics apply to the cyber domain. Fostering this effort will result in a better understanding of how military tactics and strategy fit into the cyber domain.

Future cyber strategists will emerge and pave the way for achieving cyber dominance, but analysis of concepts like key terrain must be examined. Future cyber strategists and military minds will have to break from the traditional mindset when identifying key terrain in cyberspace. At the end of the day there is no right or wrong answer as to what key terrain is, the more important point is that something must be identified as key terrain. Key terrain will not matter unless the mission is successful. Clausewitz alludes to this point, stating that "the occupation [key terrain] is nothing but a raised arm, and the position itself only a lifeless tool. … The real thrust and blow, the object, the value is *victory* in battle" (Clausewitz, 1976, p. 354).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alexander, K. B. (2007). Warfighting in cyberspace. *Joint Forces Quarterly*, 46(3), 58–61. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc? Location=U2&doc=GetTRDoc.pdf&AD=ADA518148

Allyn, D. B. (2016, November). Association of the United States Army Institute of Land Warfare hot topics forum "cyber and future readiness." Symposium conducted at the meeting of the AUSA, Arlington, VA. Retrieved from https://www.army.mil/article/177857

Applegate, S. D., Carpenter, C. L., & West, D. C. (2017). Searching for digital hilltops. *Joint Force Quarterly*, *84(1)*, 18–23. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-84/jfq-84_18-23_Applegate-Carpenter-West.pdf

Arquilla, J., & Goldman, E. O. (2014). *Cyber Analogies* (NPS-DA-14-001). Monterey, CA: Naval Postgraduate School. Retrieved from http://hdl.handle.net/10945/40037

Bodeau, D., Graubart, R., & Heinbockel, W. (2013). *Mapping the cyber terrain: Enabling cyber defensibility claims and hypotheses to be stated and evaluated with greater rigor and utility* (Report No. MTR130433). Bedford, MA: MITRE. Retrieved from http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf

Chu, P. (2016, Jan 19). Somebody keeps cutting the Bay Area's fiber-optic cables, and the FBI wonders why. *The San Francisco Business Times*. Retrieved from http://www.bizjournals.com/sanfrancisco/blog/2016/01/fiber-optic-cable-attacks-fbi-super-bowl-att.html

Clausewitz, C. V. (1976). *On War* Index edition, edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press.

Daniel, P. (2016, April). JFHQ-DODIN update. *2016 AFCEA Defensive Cyber Operations*. Symposium conducted at the meeting of AFCEA, Washington, D.C., Retrieved from http://www.disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEA-Symposium/1-LtColDaniel_JFHQ-DODIN.pdf

Department of the Army, United States Marine Corps. (2014). *Intelligence Preparation of the Battlefield/Battlespace* (ATP 2–01.3/MCRP 2–3). Washington, D.C.: Author.

Department of the Army. (2008). *Operations* (FM 3–0). Washington, D.C.: Author.

Department of the Army. (2013). *Offense and defense volume 1* (FM 3–90-1). Washington, D.C.: Author.

Department of the Army. (2011). *Unified Land Operations* (ADP 3–0). Washington, D.C.: Author

Department of the Army. (2012). *The operations process* (ADRP 5–0). Washington, D.C.: Author.

Department of Defense. (2015, Sep. 30). Cybersecurity Culture and Compliance Initiative Memorandum. Washington, D.C.: Author.

Dressler, J. (2015). *Analyzing the use of cyber in warfare at the strategic, operational, and tactical levels* (Doctoral dissertation, Rice University). Retrieved from http://hdl.handle.net/1911/88340

Franz III, G. J. (2012, August). Effective Synchronization and Integration of Effect through Cyberspace for the Joint Warfighter. *2012 AFCEA TechNetLand Forces-East Conference*. Symposium conducted in meeting of AFCEA, Baltimore, MD. Retrieved from http://www.afcea.org/events/tnlf/east12/documents/4V3EffSynchIntEffthruCybrspcforJtWarfighter_forpublicrelease.pdf

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014, August). *Green lights forever: analyzing the security of traffic infrastructure*. Paper presented at the meeting of 8th USENIX Workshop on Offensive Technologies (WOOT'14), San Diego, CA. Retrieved from https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf

Gioe, D. (2016). Can the warfare concept of maneuver be usefully applied in cyber operations? *The Cyber Defense Review*. Retrieved from http://www.cyberdefensereview.org/2016/01/14/warfare-concept/

Hearing to receive testimony on U.S. Strategic Command, U.S. Transportation Command, and U.S. Cyber Command in review of the Defense Authorization Request for fiscal year 2016 and the future years defense program: Hearing before the Senate Armed Services Committee, 114th Cong. 24 (2015) (testimony of Admiral Michael S. Rodgers). Retrieved from http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf

Hobbs, D. (2007). *Application of OCOKA to Cyberterrain*. Lancaster, PA: White Wolf Security White Paper. Retrieved from http://www.whitewolfsecurity.com/pdf/Application_of_OCOKA_to_Cyberterrain.pdf

Hollis, D. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal*. Retrieved from http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

Howell, K. (2015, Sep 16). FBI investigating severed fiber-optic cables in California, possible terrorist probe. *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2015/sep/16/fbi-investigating-severed-fiber-optic-cables-in-ca/

Internet. (n.d.) In Wikipedia. Retrieved November 14, 2016, from https://en.wikipedia.org/wiki/Internet

Kern, S. C. (2015). *Expanding combat power through military cyberpower theory* (Master's thesis). Retrieved from Defense Technical Information Center. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA621664

Kieffer, H. J. (2016). Can Intelligence Preparation of the Battlefield/Battlespace Be Used to Attribute a Cyber-Attack to an Actor? *The Cyber Defense Review*. Retrieved from http://www.cyberdefensereview.org/2016/03/22/ipb-attribution/

Lanham, M. (2012). Cyber defense planning: operating on unconventional terrain. *Army Communicator*, *37*, 7–12. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA571985

Lewis, C. (2016). People, Preparation, Process: The Three P's to Integrate Cyber at the Tactical Level. *The Cyber Defense Review*. Retrieved from http://www.cyberdefensereview.org/2016/01/19/people-preparation-process/

Libicki, M. C. (2012). Cyberspace is Not a Warfighting Domain. *I/S: A Journal of Law and Policy for the Information Society*. 8, 321–336. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc8&div=17&id=&page=

Lynn, W. J. (2010). Defending a new domain: The pentagon's cyberstrategy. *Foreign Affairs*, *89*(5), 97–108. Retrieved from http://www.jstor.org/stable/20788647

Magee, C. S. (2013). Awaiting the cyber 9/11. *Joint Force Quarterly*, 70, 76–82. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_76-82_Magee.pdf

McLane Advanced Technologies. (n.d.) Standard Army Maintenance System—Enhanced (SAMS-E). Retrieved January 16, 2017, from http://www.mclaneat.com/key-systems/sams-e/

Mills, J. R. (2012). The key terrain of cyber. *Georgetown Journal of International Affairs*, 99–107. Retrieved from http://www.jstor.org/stable/43134343

MITRE. (n.d.) Crown Jewels Analysis. Retrieved Jan 20, 2017, from https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

Pingel, T. J. (2003). Key defensive terrain in cyberspace: a geographic perspective. *Proceedings of the International Conference on Politics and Information Systems (PISTA)*. Retrieved from http://tpingel.org/documents/other/pingel.2003.pista.pdf

Raymond, D., Conti, G., Cross, T. (2014). The library of Sparta (Blackhat 2014), Retrieved from https://www.blackhat.com/docs/us-14/materials/us-14-Raymond-The-Library-Of-Sparta-WP.pdf

Raymond, D., Cross, T., Conti, G., & Nowatkowski, M. (2014). Key terrain in cyberspace: seeking the high ground. *Proceedings of 2014 6th International Conference on Cyber Conflict* (pp. 287–300). Tallinn, Estonia. doi: https://doi.org/10.1109/CYCON.2014.6916409

Riley, S. (2014). Cyber terrain": a model for increased understanding of cyber activity. (LinkedIn) [Blog Post]. Retrieved from https://www.linkedin.com/pulse/20141007190806-36149934--cyber-terrain-a-model-for-increased-understanding-of-cyber-activity

Sanger, D. E., Schmitt, E. (2015, Oct 25). Russian ships near data cables are too close for U.S. comfort. *The New York Times*. Retrieved from https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0

Sterling, B. (1992). *The hacker crackdown*. [Electronic Version]. Retrieved from http://www.mit.edu/hacker/hacker.html

Thomas, T. (2014). Creating cyber strategists: escaping the 'DIME' mnemonic. *Defense Studies, 14*(4), 370–393. doi: http://dx.doi.org/10.1080/14702436.2014.952522

United States Army Cyber Center of Excellence. (2015). *U.S. Army CCOE strategic plan*. Forward. Retrieved from http://cybercoe.army.mil/images/CyberCoE%20Documents/strategic_plan_2015_revision4_9_14_2015.pdf

United States Army Cyber Command. (2013). *The U.S. Army Landcyber white paper 2018 - 2030*. Washington, D.C.: Author. Retrieved from http://dtic.mil/dtic/tr/fulltext/u2/a592724.pdf

United States Joint Chiefs of Staff. (2009). *Joint Intelligence Preparation of the Operational Environment* (JP 2–01.3). Washington, D.C.: Author.

United States Joint Chiefs of Staff. (2010). *Department of Defense dictionary of military and associated terms* (JP 1–02). Washington, D.C.: Author.

United States Joint Chiefs of Staff. (2013a). *Cyberspace operations* (JP 3–12(R)). Washington, D.C.: Author.

United States Joint Chiefs of Staff. (2013b). *Space operations* (JP 3–14). Washington, D.C.: Author.

United States Joint Chiefs of Staff. (2017). *Joint operations* (JP 3–0). Washington, D.C.: U.S. Author.

U.S. Patriot Act of 2001. Pub L. No. 107–56. Retrieved from https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

ViaSat. (n.d.) Blue Force Tracking 2. Retrieved January 16, 2017, from https://www.viasat.com/products/blue-force-tracking-2

Welch, L. D. (2011). Cyberspace–The Fifth Operational Domain. *IDA Research Notes,* 2–7. Retrieved from https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf

Williams, B. T. (2014). The joint force commander's guide to cyberspace operations. *Joint Force Quarterly, 73*(2), 12–19. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf

Winterfeld, S. P. *Cyber IPB*. Available from SANS Institute. Retrieved from https://cyber-defense.sans.org/resources/papers/gsec/cyber-ipb-103147

ZeroFOX. (2015). ISIS compromises CENTCOM social media: Are you next? Retrieved January 16, 2017 from https://www.zerofox.com/blog/isis-compromises-centcom-social-media-next/

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California